



Tempered

**Airwall help
v3.0**

Contents

Connect to Airwall™	6
Set up an Airwall Agent or Server.....	6
Install an Airwall Agent or Server.....	6
Link my Airwall Agent or Server to an Airwall secure network.....	13
Connect to an Airwall secure network.....	18
Connect with an Apple (OSX and macOS) Airwall Agent.....	18
Connect with an iOS Airwall Agent.....	20
Connect with a Android Airwall Agent.....	21
Connect with a Linux Airwall Server.....	26
Connect with a Windows Airwall Agent or Server.....	27
Create or Edit Airwall Agent or Server Profiles.....	29
Sync an Airwall Agent or Server in Disconnected Mode.....	29
Sync Now for iOS, Android, macOS, and Windows Airwall Agents and Servers.....	29
Sync Now for Linux Airwall Servers.....	29
Change My Conductor Preferences.....	30
Change my Conductor password.....	30
Show or Hide Conductor Setup progress.....	30
I'm having trouble connecting.....	31
Linux Airwall Server or macOS Airwall Agent interface selection.....	31
Manage Airwall™	32
The Conductor Dashboard.....	32
Conductor Icon Reference.....	36
Create or Manage Dashboard Messages.....	39
Change My Conductor Preferences.....	40
Change my Conductor password.....	40
Show or Hide Conductor Setup progress.....	40
Customize the Conductor.....	41
Customize the Conductor Login page.....	41
Customize Conductor emails.....	42
Remove Conductor customizations.....	44
Manage People.....	44
Manage Conductor Admins.....	44
Import people using a CSV file.....	51
Remove people in bulk.....	53
Connect People's Devices to your Airwall secure network.....	54
Set up a People Group.....	74
Set up User Authentication.....	78
Set Times Authenticated Users can Access the Secure Network.....	78
Set up an Airwall Relay to Route Encrypted Connections.....	80
Set Up an Airwall Relay.....	81
Configure Airwall Relay rules.....	81
Set an Overlay to Automatically Manage Relay Rules.....	82
Manage Devices and Airwall Edge Services.....	82
Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers.....	82
Manage and organize with Tags.....	83
Create standard device groups.....	87
Manage devices dynamically with Smart Device Groups.....	87

Create Airwall Edge Service groups.....	96
See MAC address OUI (Manufacturer) Information for Devices.....	97
Manage Overlay Networks in Streamlined View.....	97
See Airwall Edge Service Information and Status.....	98
Airwall Edge Service Statuses.....	100
Monitor Activity and Connections.....	100
Run Network Activity Reports.....	101
Monitor Activity with Events and Alerts.....	101
Monitor Connections to your Airwall secure network.....	104
Update your Conductor and Airwall Edge Services.....	106
Manage Versions of Airwall Agents and Servers.....	106
Update Conductor Firmware.....	106
Update Airwall Gateway firmware.....	108
Replace an Airwall Gateway.....	111
Back Up your Conductor and Airwall Edge Services.....	112
Back up your Conductor.....	112
Back up Azure Airwall Gateway 300v.....	113
Conductor and Airwall Edge Service PCI Compliance.....	116
To access PCI data in the Conductor.....	117
PCI Compliance Reports.....	117

Deploy Airwall™ 117

Get Started with the Airwall Solution.....	117
Get Started using Conductor Help and Tutorials.....	118
What makes up an Airwall secure network?.....	119
What's New by Version.....	126
Definitions of Key Terms.....	149
The Airwall Solution.....	152
How to get support.....	153
Copyrights.....	154
Deploy an Airwall secure network.....	155
Deployment Checklist.....	155
Confirm your Network Settings.....	156
License a Conductor and Airwall Edge Services.....	159
Deploy and Configure a Conductor.....	165
Deploy and Configure Airwall Edge Services.....	236
Connect and Configure Devices.....	351
Create and Manage an Overlay (Protected) Network.....	355
Configure Device Trust.....	360
Set up Cloud Providers.....	364
Integrate Third-party Services.....	371
Integrate Third-party Authentication with OpenID Connect.....	372
Configure LDAP authentication on Conductor and Airwall Edge Services.....	383
Mirror traffic from your Airwall Gateways to a packet analyzer tool.....	389
Diagnostics and Troubleshooting.....	410
Diagnostic Tools.....	410
Connection Troubleshooting.....	413
Handle IP Conflicts.....	416
Update v2.1.x Airwall Edge Services for the v3.0 Conductor.....	418
Factory Reset a Conductor.....	418
Factory Reset a Virtual Conductor.....	419
Reboot an Airwall Gateway.....	419
Factory Reset an Airwall Gateway.....	419
Revoke and Reactivate an Airwall Edge Service.....	419
Troubleshoot MAP2 Protocol Issues.....	420

Measure wireless signal strength - WiFi and cellular.....	420
Advisory Notices and Product Bulletins.....	421
Advisory Notices.....	421
Product Bulletins.....	422
Airwall API.....	426
Script Repository.....	426
Tempered Software Downloads and Release Notes.....	431
Latest firmware and software.....	431
3.0 firmware and software.....	433
2.2.13 firmware and software.....	434
2.2.12 firmware and software.....	436
2.2.11 firmware and software.....	437
2.2.10 firmware and software.....	439
2.2.8 firmware and software.....	440
2.2.5 firmware and software.....	442
2.2.3 firmware and software.....	443
Cellular modem firmware.....	445
Serial drivers.....	445
Older downloads.....	446
2.2.2 firmware and software.....	446
2.2.1 firmware and software.....	447
2.1.7 firmware and software.....	449
2.1.6 firmware and software.....	450
2.1.5 firmware and software.....	451
2.1.4 firmware and software.....	452
2.1.3 firmware and software.....	453
2.1.2 firmware and software.....	454
Hotfixes.....	454
Release Notes.....	457
Latest Release Notes (v3.0).....	457
Release Notes v3.0.0.....	469
Release Notes 2.2.13.....	481
Release Notes 2.2.12 Hotfix – Conductor HF-15849.....	489
Release Notes 2.2.12 Hotfix – Conductor HF-15748.....	489
Release Notes 2.2.12.....	489
Release Notes 2.2.11 Hotfix – Conductor HF-1.....	500
Release Notes 2.2.11 Hotfix – Airwall Gateway HF-2.....	501
Release Notes 2.2.11 Hotfix – Airwall Gateway HF-1.....	501
Release Notes 2.2.11.....	502
Release Notes 2.2.10 Hotfix – Airwall Gateway HF-1.....	513
Release Notes 2.2.10 Hotfix – Conductor HF-1.....	514
Release Notes 2.2.10.....	516
Release Notes 2.2.8 Hotfix – Conductor HF-5.....	530
Release Notes 2.2.8 Hotfix – Airwall Gateway HF-3.....	533
Release Notes 2.2.8 Hotfix – Conductor HF-4.....	534
Release Notes 2.2.8 Hotfix – Airwall Gateway Hotfix-13955.....	537
Release Notes 2.2.8.....	537
Release Notes 2.2.5.....	551
Release Notes 2.2.3 Hotfix.....	553
Release Notes 2.2.3.....	554
Older Release Notes.....	563
Release Notes for Retired Hotfixes.....	641

Get Support.....	648
How to get support.....	648
Documentation Downloads.....	649
Technical Whitepapers, Best Practices, and Use Cases.....	650
Additional Resources.....	651

Connect to Airwall™

Connect your cellphone, mobile device, laptop, or server to an Airwall secure network to get access to the protected things you need to do your work. All it takes is installing the Airwall Agent or Server for your device, and then linking it to the Conductor that controls who can see those protected things on that Airwall secure network.

Before you can connect, on the device you'll use to connect, you need to:

- Install an Airwall Agent or Server on your device (laptop, tablet, or cellphone)
- Create a profile for the network you want to connect to. If you're using **Airwall Invitations** or Activation codes, this profile is created for you.

If you are not configuring the profile with **Airwall Invitations** or Activation codes, you also need to have the Conductor administrator provision and manage your Airwall Agent or Server before you can connect.



Note: If you only have one profile, when you start the Airwall Agent or Server, it automatically connects with that profile.

Set up an Airwall Agent or Server

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions.

To connect to an Airwall secure network, you need to install the Airwall Agent or Server software on the laptop, mobile device, or server that you want to connect with, and then set up a link with the secure network. Check the [Operating system requirements for Airwall Agents and Servers](#) on page 7, and find installation instructions for the device you want to connect with under [Install an Airwall Agent or Server](#) on page 6.

Install an Airwall Agent or Server

To connect to anything that is protected by an Airwall secure network on your mobile phone or laptop, you need to install an Airwall Agent or Server.

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions to connect to an Airwall secure network. Check the [Operating system requirements for Airwall Agents and Servers](#) on page 7 to make sure your laptop or mobile device can run the software.

Install an Airwall Agent or Server

On the device you are using to connect, install the Airwall Agent or Server software. Here are the places you can find the software for your device:

- Open the link in your Airwall invitation.
- Go to the store for your device and search for Airwall.
- Download and run the installation file for your device from [Latest firmware and software](#) on page 431.

If you need additional help installing the software for your platform, see the specific instructions for your device.

Once you've installed the software, you need to set it up so it can connect to the Airwall secure network. The administrator for the secure network may have sent you an Airwall Invitation or Activation code, or you may want to set up your Airwall Agent or Server manually, and request to connect to the secure network.

- [I have an Airwall Invitation](#) on page 13
- [I have an Activation Code](#) on page 14
- [I have a "Finish Setting up my account" email](#) on page 14
- [I want to request to connect](#) on page 17

You can uninstall an Airwall Agent or Server using your device's normal uninstall process.

Operating system requirements for Airwall Agents and Servers

Operating system requirements for the Airwall Solution and Airwall Teams.T

System Requirements

Please review the system requirements before installing to make sure your device can run the Airwall Agent or Server.

Microsoft Windows

The Windows Airwall Agent works on Microsoft Windows 7, 8.1, or 10, and runs on both Home and Professional versions.

Airwall only: The Windows-based Airwall Server works on Microsoft Windows Server 2008R2, 2012R2, or 2016, or later.

Apple macOS

Works on 10.14 Mojave, or 10.15 Catalina, and later.

Apple iOS

Works on iOS 13 and later. Compatible with the iPhone and iPad.

Android

Works on 6.0 (Marshmallow) and later.

Linux

Works on Ubuntu 16.04, 18.04, and 20.04, and CentOS 8, and (Airwall only) Fedora 2.7.

Raspbian (Raspberry Pi)

Raspbian 9 (Stretch) or 10 (Buster)

RPi4/Ubuntu ARM64 (Raspberry Pi)

Raspbian 10 (Buster)

Apple (OSX and macOS): Install and configure an Airwall Agent

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You must be an administrator of the computer to install and configure the Airwall Agent.



Note: Download the macOS/OSX installation files from the [Tempered Software Downloads and Release Notes](#) on page 431 Software Downloads section of Airwall help.



Important: In v2.2 and earlier, you may be required to install a TAP device driver. In earlier versions, the TAP driver's certificate may display a developer other than Tempered. If this occurs, you can safely click **Allow** and continue with your installation.

Once the installation is complete, the application starts automatically.

To install and configure manually:

1. To install the Airwall Agent locate the files you downloaded, double-click on them to run the installer, and follow the prompts.
2. Left-click the Tempered icon in the macOS menu bar
3. Select **Configure**.
4. On the **Airwall Configuration** page, do the following:
 - a) Select the plus (+) to add a new profile.
 - b) Under **Conductor**, enter the IP address or host name of your Conductor.
 - c) Under **Port**, use the default port setting of *8096*, unless your Airwall secure network administrator has told you to use a different port.
 - d) If you have an Activation code, under **Invitation**, enter the code. If you don't have a code, copy down or screenshot your **Device ID** and send to your administrator to activate your account.



Note: **Device ID**, **Overlay Device IP** and **Overlay Netmask** are read-only and configurable from the Conductor.

- e) Select **Save**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.



Note: You may need to stop and restart the Airwall Agent to allow it to connect to the Conductor. Left-click the Tempered icon in the menu bar and select **Stop Airwall** to disconnect or **Start Airwall** to connect.

For information on using your macOS Airwall Agent, see [Connect with an Apple \(OSX and macOS\) Airwall Agent](#) on page 18.

Apple iOS: Install and configure an Airwall Agent

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for iOS from Apple's App Store.



Note: If you received an invite, follow the instructions in the email to install and configure your Airwall Agent. The instructions below are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Apple Store: <https://itunes.apple.com/US/app/id1233852249>.
2. Open the Apple iOS Airwall Agent.
3. From the menu, tap **Profiles**. Tap + to add a new profile.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it at the bottom.
6. Tap **ADD**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Apple iOS Airwall Agent, see [Connect with an iOS Airwall Agent](#) on page 20.

Android: Install and configure an Airwall Agent

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for Android from the Google Play Store. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.



Note: If you received an invite, follow the instructions in the email to install and configure your Airwall Agent. The instructions below are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Google Play store: <https://play.google.com/store/apps/details?id=com.temperednetworks.hipclient>
2. Open the Android Airwall Agent.
3. Add a new profile:
 - **v3.0 and later** – Scroll down to **Select Profile**, tap **MANAGE**, and then tap +.
 - **v2.2.12 and earlier** – From the menu, tap **Profiles**, and then tap +.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it.
6. Tap **ADD**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Android Airwall Agent, see [Connect with a Android Airwall Agent](#) on page 21.

Linux: Install and configure an Airwall Server

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Server for your Ubuntu, Centos, or Fedora Linux server from the administrator for your Airwall secure network, or from [Latest firmware and software](#) on page 431. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.



Note:

- For pre-3.0 versions, replace airsh with airctl.
- For pre-2.2.3 versions, see [pre-2.2.3 help](#).

1. Install the Linux Airwall Server package for your version of Linux. If your secure network administrator has not provided you with a download, you can download the package you need from [Latest firmware and software](#) on page 431.
 - **For CentOS 7 or 8 or Fedora 3.3:** sudo rpm -i <CentOS or Fedora install package>
 - **For Ubuntu 16.04, 18.04, or 20.04:** sudo dpkg -i <Ubuntu 16 or 18 package>
2. Create a profile: sudo airsh profile create name=<profile name> conductor=<conductor_url> [act=activation_code].
You can optionally enter an Airwall Invitation activation code.
3. Make a profile the active one: sudo airsh profile activate <profile name or number>
4. Start the service: sudo airsh service start.



Note: If the service is already running, enter sudo airsh service restart to stop and start the service.

If you've used an Airwall Invitation or Activation code, once the Airwall Server is recognized by the Conductor, you should be able to start connecting to protected resources on the Airwall secure network. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on getting your Device ID, or using your Linux Airwall Server, see [Connect with a Linux Airwall Server](#) on page 26. For more Airshell commands, see [Linux Airwall Server Airshell commands](#) on page 309.

airctl Reference (pre-v3.0)

Here are the airctl commands available. You can see commands by typing airctl reference.

You use the airctl command line to see details on Linux or Raspberry Pi Airwall Agent or Server. On your Linux or Raspberry Pi device, open a terminal window, and type airctl or sudo aircrl, followed by the desired command.

```
profile details <profile name>
details=<profile-details>

profile modify <profile
name> [new_name=<string>]
[conductor=<addr:port>]
[network=<interface | auto>]
[invitation=<invitation>]
[log_level=<info | warn | error |
debug | trace>] [sys=<sys-impl>]
[activate] details=<profile-details>

profile activate <profile name>
[sys=<sys-impl>] profile_name=<string>

profile create <new profile
name> [allow_rename=<boolean>]
conductor=<addr:port>
```

Show all or some of the details of an Airwall Agent or Server profile. Instead of entering a profile name, you can get details on the currently-active profile by entering airctl profile details --active.

Modify a profile. For example, to change the log level to debug for a profile named myprofile, you would enter: airctl profile modify myprofile log_level=debug.

```
[network=<interface | auto>]
[invitation=<invitation>] [sys=<sys-
impl>] [activate] details=<profile-
details> profile_name=<string>

profile delete <profile name> <no
additional result data>

profile rename <profile
name> new_name=<string>
profile_name=<string>

service start [sys=<sys-impl>] <no
additional result data>

service stop [sys=<sys-impl>] <no
additional result data>

service restart [sys=<sys-impl>]
[full] <no additional result data>

service status running=<bool>
conductor=<bool> tunnel=<bool>

list interfaces
_interfaces=<_interfaces>

list profiles _profiles=<profile-
list> current_dir=<string>
current_name=<string>
root_dir=<string>

list versions hipapp_version=<string>
hipctl_version=<string>

list log <profile name>
[max_lines=<integer>] [log_level=<info
| warn | error | debug | trace>]
_log=<_log> profile_name=<string>

support reset <profile name> support
reset=<string>

support bundle output=<string>
```

Microsoft Windows or Windows Server: Install and configure an Airwall Agent or Server

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent or Server for Windows from the administrator of your Airwall secure network, or download the latest installation files from [Latest firmware and software](#) on page 431. Once installed, you configure a profile on the Airwall Agent or Server to link to the Airwall secure network.



Note: You can start and stop the Airwall Agent or Server service as needed. Keep in mind when an Airwall Agent or Server service is stopped, you won't be able to connect to anything on the protected network.

To install and configure the Windows Airwall Agent or Server:

1. Log into your Windows computer as an administrator.
2. Download and install the Windows Airwall Agent or Server from [Latest firmware and software](#) on page 431.



Note: If you are asked to install the TAP-Windows Provider as part of the installation procedure, click **Install** when prompted.

3. Once the installation is complete, the Airwall Agent or Server starts automatically.

4. Right-click the Tempered icon in the Windows System Tray

5. Select **Configure**

6. In the **Configure** window, do the following:

- Enter the IP address or host name of your Conductor. The default port setting is **8096**. If you have an activation code, enter it here.



Note: The **Device ID**, **Overlay Device IP**, and **Overlay Netmask** fields are read-only and configurable from the Conductor.

- Click **OK**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent or Server is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Windows Airwall Agent or Server, see [Connect with a Windows Airwall Agent or Server](#) on page 27.



Note: You may need to stop and restart the Airwall Agent or Server to allow it to connect to the Conductor. Right-click the Tempered icon in the Windows System Tray and select **Stop** to suspend the service or **Start** to resume.

Raspbian and RPi4/Ubuntu ARM64 – Install the Airwall Server

To connect to Airwall Teams, install the Raspberry Pi Raspbian or RPi4/Ubuntu ARM64 Airwall Server on your device.

Before you begin, check the [Operating system requirements for Airwall Agents and Servers](#) on page 7 for your Raspberry Pi device.

- On your Raspberry Pi, open the email you received and select **Click here to confirm this mail**.
- Fill in the **Create Account** form: Enter your name and create an Airwall Teams account password.
- Read and agree to the terms: Check **I have read and agree to all terms in the end user licensing agreement**, and click **Submit**.

The screenshot shows a dark-themed web form titled "Create your free Airwall Teams account". Below the title is the tagline "simple, fast, private networks". The form contains several input fields: "first name*", "last name*", "company*", "title", "intended use" (a dropdown menu set to "Select one"), "phone number*" (with "555-555-5555" entered), "email*", "password*", and "confirm password*". At the bottom left is a checkbox labeled "I have read and agree to all terms in the end user licensing agreement". A blue "create your account" button is at the bottom right.

- Under Step 1, click the link to download the installation file for your Raspberry Pi version. Click **More Downloads** if your installation type isn't shown.

5. Install the Airwall Server package for your version of Raspberry Pi. You can copy and paste the commands from the install page:

The screenshot shows a software interface titled "Activate RPi_arm64". It has two main sections: "Step 1: Install an Airwall agent or server" and "Step 2: Activate".

Step 1: Install an Airwall agent or server

- Download an Airwall agent to **RPi_arm64** and install it. Then return here to activate it.
- Options: Android Airwall agent, Mac Airwall agent, iOS Airwall agent, Windows Airwall agent, Ubuntu 18.04 / 20.04 Airwall server, CentOS 8 Airwall server, RPi4/Ubuntu ARM64 Airwall server, Raspbian Airwall server.
- Less Downloads... Need help installing?
- To install the Linux Airwall server, enter the following commands in your Linux terminal:
(this requires root privileges)

```
wget --output-document=/tmp/hipserver.deb https://teams.tempered.io/download/clients/airwall-2.2.10.Ubuntu18.arm64.deb
sudo ACCEPT_EULA=y dpkg -i /tmp/hipserver.deb
```

Step 2: Activate

- If you have your Airwall server installed, use your terminal to activate it with the command below.
- sudo airctl profile create "Airwall Teams" conductor=tn-online-00.tempered.netw ork:8096 invitation=a1326ce9efeb activate

Terminal Output:

```
pi@raspberrypi: ~ wget --output-document=/tmp/hipserver.deb https://teams.tempered.io/download/clients/airwall-2.2.10.Ubuntu18.arm64.deb
--2021-02-08 15:35:23-- https://teams.tempered.io/download/clients/airwall-2.2.10.Ubuntu18.arm64.deb
Resolving teams.tempered.io (teams.tempered.io)... 52.89.96.81, 52.10.166.129
Connecting to teams.tempered.io (teams.tempered.io)|52.89.96.81|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://s3.amazonaws.com/temperedclients/airwall-2.2.10.Ubuntu18.arm64.deb [following]
--2021-02-08 15:35:23-- https://s3.amazonaws.com/temperedclients/airwall-2.2.10.Ubuntu18.arm64.deb
Resolving s3.amazonaws.com (s3.amazonaws.com)... 52.216.141.246
Connecting to s3.amazonaws.com (s3.amazonaws.com)|52.216.141.246|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3527528 (3.4M) [binary/octet-stream]
Saving to: '/tmp/hipserver.deb'

/tmp/hipserver.deb          100%[=====]   3.36M    769KB/s   in 5.0s

2021-02-08 15:35:29 (685 KB/s) - '/tmp/hipserver.deb' saved [3527528/3527528]
```

You can also manually install by entering:

Raspbian:

```
wget --output-document=/tmp/airwall.deb https://teams.tempered.io/download/clients/airwall_2.2.10.Raspbian9.armhf.deb
```

RPi4 Ubuntu ARM64:

```
wget --output-document=/tmp/airwall.deb https://teams.tempered.io/download/clients/airwall-2.2.10.Ubuntu18.arm64.deb
```

- Accept the EULA using sudo ACCEPT. Again, you can copy from the install page:

```
pi@raspberrypi:~ $ sudo ACCEPT_EULA=y dpkg -i /tmp/hipserver.deb
(Reading database ... 90460 files and directories currently installed.)
Preparing to unpack /tmp/hipserver.deb ...
Unpacking airwall (2.2.10) over (2.2.10) ...
Setting up airwall (2.2.10) ...
updating profile /opt/tmw/profiles/profile1
updating profile /opt/tmw/profiles/profile-123123
updating profile /opt/tmw/profiles/.factory
```

You can also manually enter the command:

```
sudo ACCEPT_EULA=y dpkg -i /tmp/airwall.deb
```

- Create a profile and activate your connection by copying and pasting the activation command from the install page.

```
pi@raspberrypi:~ $ sudo airctl profile create 'Airwall Teams' conductor=ttn-online-00.tempered.network:8096 invitation=50610f8bb321 activate
profile_dir: profile-123124
profile_name: Airwall Teams
network: auto
deviceID:
overlay_device_ip:
overlay_mask:
invitation: 50610f8bb321
conductor: ttn-online-00.tempered.network:8096
log_level: info
profile_name: Airwall Teams
```

You can also manually activate by entering:

```
sudo airctl profile create <profile name> conductor=<conductor>
    invitation=<invite code> activate
```

- Start the service my entering:

```
airctl service start
```

 **Note:** If the Airwall service is already running, it may not activate a new profile without first stopping and starting the service.

- Return to the Airwall Teams website and click **Activate**. Copy the command under **Step 2: Activate**. You will use this command to activate the Airwall Server.
- Paste the command into a terminal window, and press **Enter** to activate your Airwall Server.
- Wait for the Airwall Server to activate. When complete, you'll get a message that your Airwall Server has been activated.

Click **Look around** to close the activation window. Find your device in the device list on the left to verify you are connected. You can also check in a terminal by typing the following:

```
sudo airctl service status
```

In the output, look for the line `conductor=true`, which means you are connected to your Airwall Teams network.

Link my Airwall Agent or Server to an Airwall secure network

Once you've installed the Airwall Agent or Server software, you can link it to one or more Airwall secure networks.

 **Tip:** For the best experience for you and the administrator for the secure network you're linking to, ask your Airwall administrator to send you an Airwall Invitation or **Activation Code**.

Click the section below for how were you invited to an Airwall secure network.

I have an Airwall Invitation

Connect your Airwall Agent or Server to an Airwall secure network with an Airwall Invitation.

- Install an Airwall Agent or Server on page 6.
- After you've installed the software, open the Airwall invitation on the same device, and click **Activate**.
- Open the Airwall Agent, and tap **Get Started**.
- From the menu, tap **Profiles**.

5. Select the profile created when you activated your invitation, and slide the toggle to **On**. It may take a few minutes for your device to complete activation, and then it will show you are connected to the Conductor.

You can now turn on the Airwall Agent or Server profile when you need to access protected assets. See [Connect to an Airwall secure network](#) on page 18.

I have an Activation Code

Connect your Airwall Agent or Server to an Airwall secure network with an Activation code.

How to connect to an Airwall secure network when you've received an Activation code.

1. [Install an Airwall Agent or Server](#) on page 6.
2. To activate an Airwall Agent, see [Set up my Airwall Agent Manually](#) on page 17.
To activate an Airwall Server, see [Set up my Airwall Server Manually](#) on page 17.

I have a "Finish Setting up my account" email

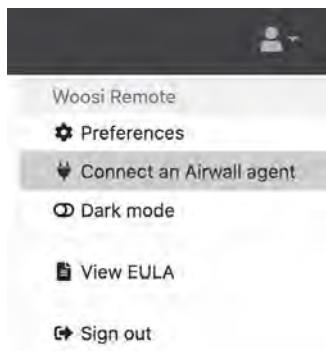
Connect your Airwall Agent or Server to an Airwall secure network from the "Finish setting up my account" email.

How to connect to an Airwall secure network when you received an email saying "Finish setting up your account."

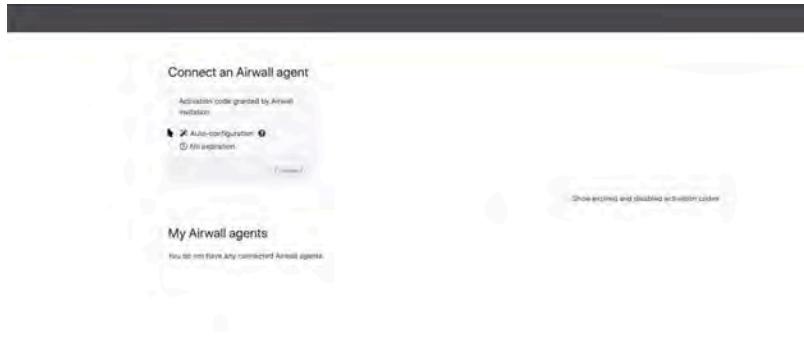
1. [Install an Airwall Agent or Server](#) on page 6.
2. From the computer, cellphone, or tablet that you want to connect to this Airwall secure network, open the "Finish setting up your account" link in the email.
3. Enter and confirm a password, then click **Change my password**. If the token is not filled in, either click the link in the email that has the token, or copy the token from the email and paste in the top box.



4. If you're not on the **Connect an Airwall Agent** page, click your profile icon in the upper right and select **Connect an Airwall Agent**.



5. On the **Connect an Airwall Agent** page, under **Activation code granted** box, click **Connect**.



6. Follow the **Connect an Airwall Agent** steps to install the Airwall Agent or Server for your computer or mobile device.

If your computer or mobile device isn't shown, open **More downloads** to find the correct version to install.

7. When the Airwall Agent or Server is installed, come back to the **Connect an Airwall Agent** page, and click **Activate**. You may need to give permission for the Airwall Agent or Server to make changes to your program.

Activation creates a profile in your Airwall Agent or Server that you can use to access resources on the Airwall secure network. You can have multiple profiles if you need to connect to different secure networks. See [Create or Edit Airwall Agent or Server Profiles](#) on page 29.

Note: If you don't have an Activation code, you can select **Request a Connection** to send the Airwall secure network administrator a request to add you to the network.

- When it's finished, you'll see a confirmation that your profile has been activated.

Airwall

Activated profile for: cond.example.com

OK

Connect an Airwall agent

Step 1: Log into Conductor

Ensure you are logged into Conductor on the device you want to connect. If you are not, please log out and log in again on the device you wish to connect to Conductor.

Step 2: Install an Airwall agent

Download an Airwall agent installation package to your computer or mobile device and install it. Then return here to activate it.

Mac Airwall

Need help installing?

+ More downloads

Step 3: Activate ✓

If you have your Airwall agent installed, you're ready to continue.

Connected!

Close

Airwall agent	Model	Status	Overlay IP
j.banks's Airwall-Mac (BC838EE8B090) BH@40130#BC838EE8B070	Airwall-Mac v2.2.3	192.168.1.51	NAT

- Select **Close** to close this page. The **Connect an Airwall Agent** page now shows your active Airwall Agents and Servers, and their status:

My Airwall agents

Airwall agent	Model	Status	Overlay IP
j.banks's Airwall-Mac (BC838EE8B090) BH@40130#BC838EE8B070	Airwall-Mac v2.2.3	192.168.1.51	NAT

10. Click the arrow to the left of your Airwall Agent or Server to see what resources (Remote devices) you have access to:

My Airwall agents			
Airwall agent	Model	Status	Overlay IP
w.wildwood's Airwall-Mac BH@40130#99983D7421C3	Airwall-Mac v2.2.3	192.168.1.11 Up	NAT
	Remote devices Overlay IP		
nwcu conductor	172.16.26.30		
test-gw	172.16.0.250		

You can now use the Airwall Agent or Server to connect to these resources on the Airwall secure network. For how to start and stop your secure connection or change profiles, see [Connect to an Airwall secure network](#) on page 18.

I want to request to connect

Request to connect your Airwall Agent or Server to an Airwall secure network.

You can manually set up your Airwall Agent or Server by creating a profile and entering the Conductor address for the Airwall secure network. You can get the Conductor address from the administrator for the secure network. When you're finished setting up your profile , the first time you attempt to connect, the Airwall secure network administrator gets a request from you to allow you to connect and then configure the resources you have access to.

Set up my Airwall Agent Manually

1. Open the Airwall Agent, and tap Get Started.
2. From the menu, tap **Profiles**.
3. Tap the plus (+) sign.
4. Enter a name for your profile.
5. Enter the Conductor address (URL or IP address).
6. Tap **Add**.
7. On the main page of your Airwall Agent, select the new profile, and slide the toggle to open the connection.
8. If you have an Activation Code, enter it in the **Activation Code or Invitation** box.

If you don't have an Activation Code, send your Conductor administrator your device ID (shown on the profile page) and request they provision your device. Leave the Airwall Agent profile on while your administrator finds and provisions your device.

If you've connected with an Activation code, you will be able to connect right away. If you have requested your device be provisioned, you will have access once the Conductor administrator provisions your device.

When your Airwall Agent shows you're connected to the Conductor, and you can reach assets in the Airwall secure network on your device. See [Connect to an Airwall secure network](#) on page 18.

You can now turn on the Airwall Agent profile when you need to access protected assets.

Set up my Airwall Server Manually

Set up a Windows Airwall Server manually

1. Open the Airwall Server, and from the menu, click **Configure**.
2. At the bottom of the left side, click the plus (+).
3. Enter your password to allow changes on your device.
4. Enter a name for the new profile.
5. Enter the Conductor URL or IP address provided by your Conductor administrator, and click **OK**.
6. On the main page of your Airwall Server, select the new profile.
7. Click the gear icon at the bottom of the profile list, and select **Make Active**.
8. Send your Conductor administrator your device ID (shown on the profile page) and request they provision your device. Leave the Airwall Server profile on while your administrator finds and provisions your device.

Set up a Linux Airwall Server manually

1. To create a new profile and activate with an Activation code, enter:

```
sudo airctl profile create <profile_name> conductor=<conductor_url>
  invitation=<activation_code>
```

For example:

```
sudo airctl profile create MyProfile conductor=cond.example.com
  invitation=45k234k678k901k
```

2. To modify an existing profile and activate with an Activation code, enter:

```
sudo airctl profile modify <profile_name> conductor=<conductor_url>
  invitation=<activation_code>
```

For example:

```
sudo airctl profile modify MyProfile conductor=cond.example.com
  invitation=45k234k678k901k
```

Once the Conductor administrator provisions your device, your Airwall Server shows you're connected to the Conductor, and you can reach assets in the Airwall secure network with your device.

You can now turn on the Airwall Server profile when you need to access protected assets. For more information, see [Connect to an Airwall secure network](#) on page 18.

Connect to an Airwall secure network

Once you've installed and linked your Airwall Agent or Server, you can then start and stop it at any time to connect and disconnect from the Airwall secure network.



Note:

- You can use your Airwall Agent or Server to connect to other Airwall secure networks. Just set up a new profile for each one you need to connect to. For information on how, see [Create or Edit Airwall Agent or Server Profiles](#) on page 29
- The Airwall Agent or Server does not disable the wired or wireless interfaces of your device. For example, if you are running an Airwall Agent, you can at the same time be connected to the Internet wirelessly and the corporate network via a wired connection.

Connect with an Apple (OSX and macOS) Airwall Agent

How to connect to an Airwall secure network with an OSX/macOS Airwall Agent.

Connect to the Airwall secure network

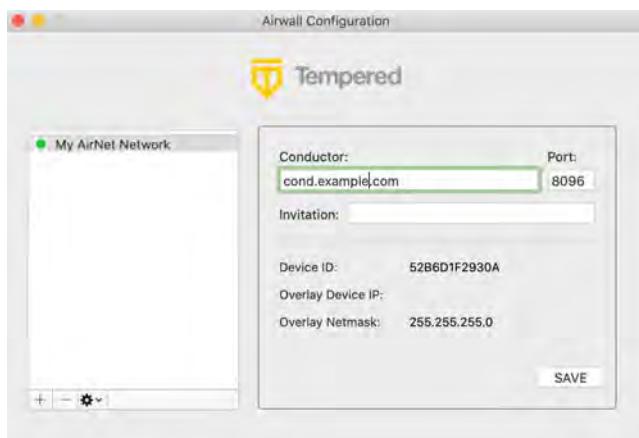
In the macOS top bar, select the Tempered shield , and select **Start Airwall**.

Manage Profiles

To manage your profiles, start the macOS Airwall Agent, click the Tempered shield , and then select **Configure** to open the Configure page.

- **To create a new profile**, From the menu, select **Configure**, and click the plus (+)  .
- **To switch profiles**, If the profile you want has a solid green dot to the left, it's already the Active profile. If it doesn't, select the profile you want to use, select the gear or triple dot icon (depending on your version) below the

profile list, and select **Make Active**. The Agent disconnects and then connects with the new profile. This can take a few minutes.

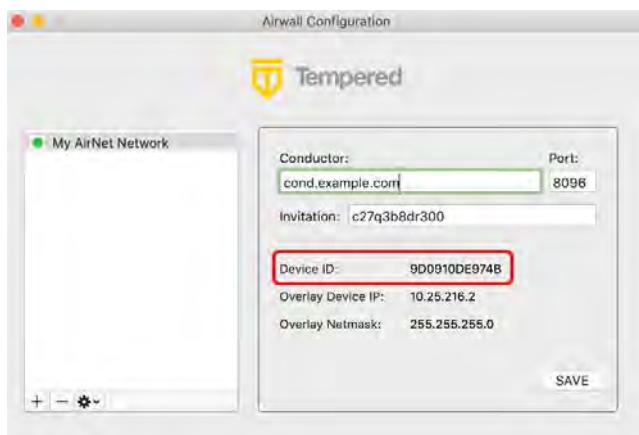


- **To edit an existing profile**, Select a profile to edit, edit the details on the right, then select **SAVE**.
- **To delete a profile**, Select it and below the list, click -.

Find your device ID

If you're still not connected, you may need to provide your device ID to the administrator for your Airwall secure network.

1. Open the macOS Airwall Agent.
2. In the macOS top bar, click the Tempered shield , and then select **Configure**.
3. Select the profile you are using to connect to the Airwall secure network.
4. On the right, under **Device ID** is the information you need to provide to your Airwall secure network administrator.



Check your Connection

There are two ways to check your connection:

- In the macOS top bar, look for the status dot next to the Tempered shield :
 - No dot or green dot: Connected to the active profile.
 - Dark grey dot: Service stopped.
 - Red dot: No connection.
 - Purple dot: In Disconnected mode (connected to resources but not the Conductor.) See [Sync an Airwall Agent or Server in Disconnected Mode](#) on page 29

- Select the shield icon and select **Configure** to see which profile is active on the **Airwall Configuration** page (shown by the green dot):

Disconnect from the Airwall secure network

In the macOS top bar, select the Tempered shield , and select **Stop Airwall**.

Connect with an iOS Airwall Agent

How to connect to an Airwall secure network with a iOS Airwall Agent.

Connect to the Airwall secure network

Open the iOS Airwall Agent, and under **Profile**, tap the slider to slide to the right to connect.

Manage Profiles

- **To create a new profile**, From the menu, tap **Profiles**. Tap + to add a new profile.
- **To switch profiles**, tap the **Profile** tab, tap the profile you want to switch to. If you are asked if you want to disconnect and switch to the profile selected, tap **Yes**.



Note: If the profile you want is displayed, it's the Active profile.

- **To edit an existing profile**, From the menu, tap **Profiles**, tap **Edit**, and select a profile to edit.
- **To delete a profile**, touch the profile name, slide right to left and tap **Delete**.

Find your device ID

If you're still not connected, you may need to provide your device ID to the administrator for your Airwall secure network.

1. In the iOS Airwall Agent, switch to and connect the profile you want to use.
2. Tap the Info tab at the bottom of the page. The Device ID to provide to your Airwall secure network administrator is on this page.

Check your Connection

Open your iOS Airwall Agent. Check that:

- Under **Profile**, the correct profile is open, and that the slider is to the right and green.

- Under **Status**, both **Connected to Conductor** and **Connected to Devices** are solid green.
This example shows that you're connected to the Conductor and Devices.



A **Grey dot** means no connection or not connected.

Disconnect from the Airwall secure network

Open the iOS Airwall Agent, and under **Profile**, tap the slider to slide to the left to disconnect.

Connect with a Android Airwall Agent

How to connect to an Airwall secure network with a Android Airwall Agent.

Connect to the Airwall secure network

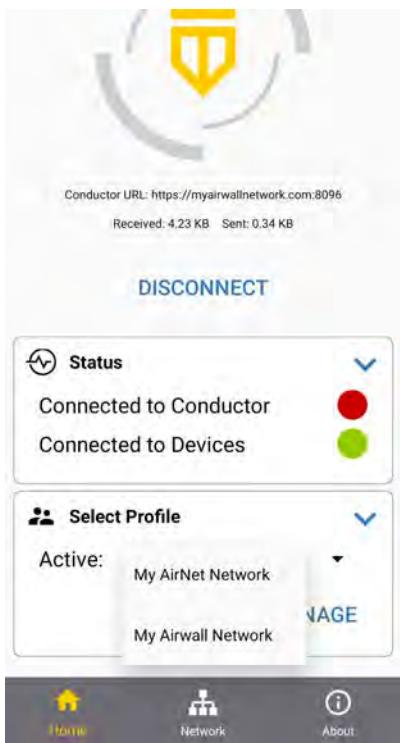
- v3.0 and later** – Tap **CONNECT**.
- v2.2.12 and earlier** – Open the Android Airwall Agent, and under **Profile**, tap the slider to slide to the right to connect.

Manage Profiles

- **v3.0 and later –**

- **To create a new profile** – Scroll down to **Select Profile**, tap **MANAGE**, and then tap **+**.
- **To switch profiles** – Under **Select Profile**, tap the down arrow next to the active profile name, and select the profile you want to switch to.

 **Note:** If the profile you want is already displayed, it's already the Active profile.



- **To edit an existing profile** – Scroll down to **Select Profile**, tap **MANAGE**, tap the three dots next to the profile you want to edit, and tap **Edit**. Or, tap and hold a profile to edit. Tap **Save** when done.
- **To delete a profile** – Scroll down to **Select Profile**, tap **MANAGE**, tap the three dots next to the profile you want to edit, and then tap **Delete**.

- **v2.2.12 and earlier –**

- **To create a new profile** – From the menu, tap **Profiles**. Tap + to add a new profile. Enter the information needed and tap **Add**.
- **To switch profiles** – Under **Profile**, tap the active profile name, and select the profile you want to switch to.



Note: If the profile you want is already displayed, it's the Active profile.



- **To edit an existing profile** – From the menu, tap **Profiles**. Tap and hold a profile to edit. Tap **Save** when done.
- **To delete a profile** – From the menu, tap **Profiles**. Tap and hold a profile to edit. At the bottom, tap **Delete**.

Find your device ID

If you're still not connected, you may need to provide your device ID to the administrator for your Airwall secure network.

1. In the Android Airwall Agent, switch to and connect with the profile you want to use.
2. Find your device ID:

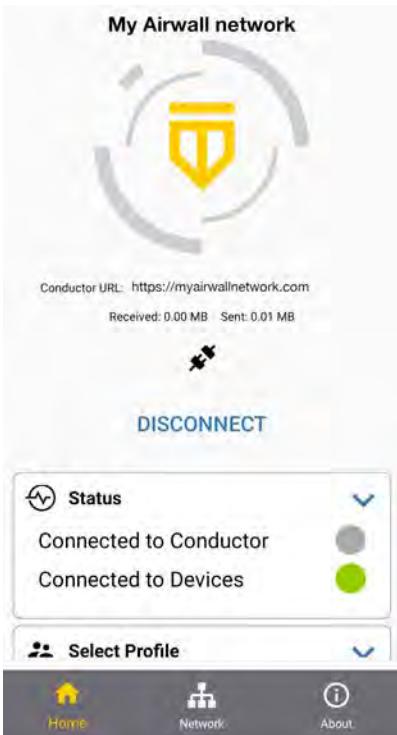
- **v3.0 and later** – At the bottom, tap **Network**. Copy and give your Airwall secure network administrator the **UID**.
- **v2.2.12 and earlier** – Tap the top left menu, and then tap **Info**. Find the **Device ID** to provide to your Airwall secure network administrator at the top of this page.

Check your Connection

Open your Android Airwall Agent. Check that:

- On v3.0 and later, check:
 - Under **Select Profile**, the correct profile is active.
 - Under **Status**, check that **Connected to Devices** shows connected (green).

 **Note:** If your Airwall secure network administrator has your device set to Disconnected mode, your **Connected to Conductor** status shows as disconnected most of the time, but you'll still have access to devices. See [Sync an Airwall Agent or Server in Disconnected Mode](#) on page 29.



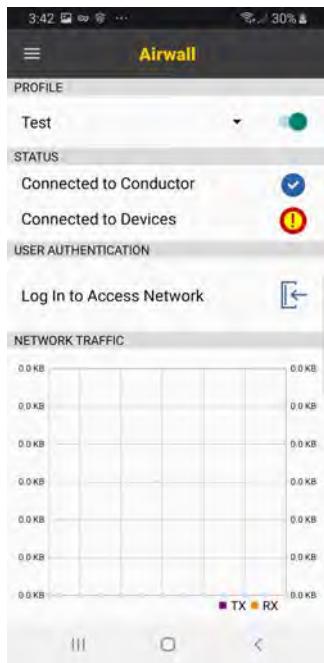
- Tap **Networks**. The network details overlay view shows your connection to devices, and the underlay shows connection to Airwall Gateways that manage secure connections to the devices.

- On v2.2.12 and earlier, check:
 - Under **Profile**, the correct profile is active.
 - The slider next to the profile is to the right and green
 - Under **Status**, both **Connected to Conductor** and **Connected to Devices** are blue checks.
- This example shows that you're connected to the Conductor, but not yet connected to Devices.



- **In v2.2.12 and earlier**, here are some other statuses you may see:
 - **Red check**: You can reach the Conductor, but your administrator has not yet accepted your request to connect.
 - **Grey dot**: No connection, or not connected.

- **Red exclamation point:** You need to log in. Tap the exclamation point, or under User Authentication, tap the Log in icon to log in.



Disconnect from the Airwall secure network

- **v3.0 and later** – Open the Android Airwall Agent, and tap **DISCONNECT**.
- **v2.2.12 and earlier** – Open the Android Airwall Agent, and under **Profile**, tap the slider to slide to the left to disconnect.

Connect with a Linux Airwall Server

You manage your Linux Airwall Server profiles and connections on the command line using Airshell (`airsh`). You can currently substitute `airctl` for `airsh` in most of these commands, but `airctl` will be phased out in a future release.

In addition to the commands below, you can enter `sudo airsh help tree` to see available commands. Not all Airshell commands are supported on a Linux Airwall Server. See [Linux Airwall Server Airshell commands](#) on page 309.

Connect and Disconnect from the Airwall secure network

- To connect to the active profile, enter:

```
sudo airsh service start
```

- To disconnect, enter:

```
sudo airsh service stop
```

- If the service is already started, restart by entering:

```
sudo airsh service restart
```

Manage Profiles

- **To create a new profile**, run: `sudo airsh profile create name=<new profile name> conductor=<conductor_url> [act=<activation_code>]`
- **To switch profiles**, run: `sudo airsh profile activate <profile name or number>`

- **To edit an existing profile**, run: `sudo airsh profile modify <profile name or number> [name=<new_name>] [conductor=<conductor_url>] [act=<activation_code>] [log_level=<info | warn | error | debug | trace>]`
- **To delete a profile**, run: `sudo airsh profile delete <profile name or number>`

Find your device ID

If you're still not connected, you may need to provide your device ID to the administrator for your Airwall secure network. To get your device ID, enter:

```
sudo airsh profile list verbose <profile_name>
```

Check your Connection

To check your connection, enter:

```
sudo airsh status
```

Check your WiFi connection

To check your WiFi connection (when a WiFi NIC is available), enter:

```
sudo airsh status wifi
```

Follow the log to troubleshoot your Linux Airwall Server

To watch the log file, enter:

```
sudo airsh log follow
```

Connect with a Windows Airwall Agent or Server

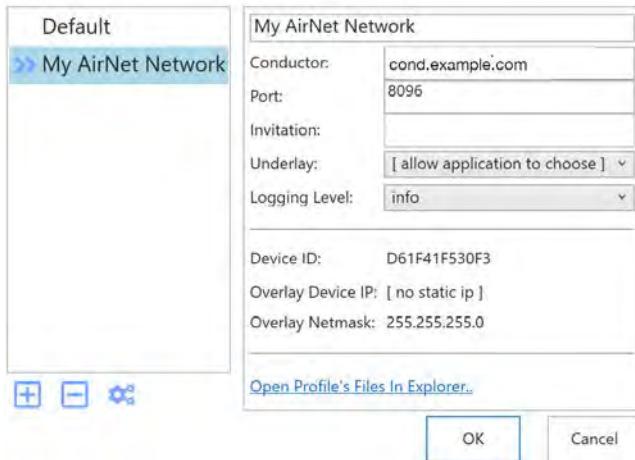
How to connect to an Airwall secure network with a Windows Airwall Agent or Server.

Connect to the Airwall secure network

Open the Airwall Agent or Server. If it doesn't connect automatically, on the Windows taskbar, right-click the Tempered icon, and select **Start**.

Manage Profiles

- **To create a new profile**, from the Control Panel, click the gear , and click + to add a new profile.
- **To edit an existing profile**, from the Control Panel, click the gear, and select a profile to edit it.
- **To switch profiles**:
 1. From the Control Panel, click the gear. (You can also right-click the Airwall Agent icon, and select **Configure**.)
 2. On the **Configure** page, if the profile you want has the double arrows  to the left, it's already the Active profile. If it doesn't, select the profile you want to use.
 3. Click the gears icon  below the profile list, and choose **Make profile active**.
 4. Select **OK**. The Agent disconnects and then connects with the new profile. This can take a few minutes.
- **To delete a profile**, select it and click -.



Find your device ID

If you're still not connected, you may need to provide your device ID to the administrator for your Airwall secure network. You can find and copy it from the top of the **Airwall Agent/Server Control panel**. Click the icon on the right to copy the device ID:



Check your Connection

1. Open the Airwall Agent or Server.
2. At the top, you will see either **Stopped** or **Running**.
 - a) If it's **Stopped**, the profile is still loading and connecting.
 - b) If it's **Running**, the profile is running, but not necessarily connected.
3. When it says **Running**, just to the right, select the overlay icon (gear with a question mark).
4. Under **Conductor and Authentication**, check to see your connection status next to **Conductor**. If you are connected, it has a green dot and says **Connected**.
5. You can also see the resources this profile gives you access to under **Network Policies and Peer Devices**:
 - a) To see the devices you have access to, open the **Overlays** tab.
 - b) To see the **Airwalls** you have access to, open the **Underlay** tab.
6. To refresh the list, select **Ping opened network**.

Disconnect from the Airwall secure network



Right-click the Airwall Agent icon, and select **Stop**.

Create or Edit Airwall Agent or Server Profiles

How you configure your Airwall Agent or Server profile varies by which version you've installed.

Go to [Connect to an Airwall secure network](#) on page 18 and select your platform to get information on creating and editing profiles, as well as connecting and disconnecting to an Airwall secure network using your Airwall Agent or Server.

Sync an Airwall Agent or Server in Disconnected Mode

If your Airwall secure network administrator has set your Airwall Agent or Server to Disconnected Mode, it will synchronize with the Conductor at regular intervals, and should not affect your connection to the resources you need to access on the Airwall secure network. If you are having issues, you can manually sync with the Conductor.

Sync Now for iOS, Android, macOS, and Windows Airwall Agents and Servers

- **For mobile Airwall Agents** – Open your mobile agent, and on the Home page, under **Disconnected Mode**, select **Sync Now**.

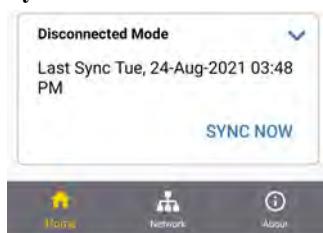


Figure 1: iOS and Android Airwall Agent Sync Now

- **For desktop agents** – Open the Airwall Agent or Server menu by clicking the icon, hover over **Disconnected Mode** and select **Synchronize Now**.

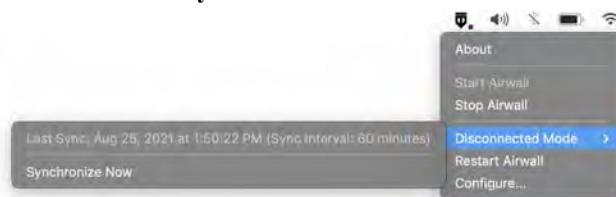


Figure 2: macOS Sync Now



Note: If you don't have the Disconnected Mode pane on your home page, your Airwall Agent or Server is not in Disconnected mode. For assistance troubleshooting your connection, see [I'm having trouble connecting](#) on page 31 or contact your Airwall secure network administrator.

Sync Now for Linux Airwall Servers

If you need to manually sync your Airwall Server with the Conductor, open Airshell and enter the `conductor sync` command:

1. Make sure the Linux Airwall Server is started:

```
sudo systemctl start airwall
```

2. Get into Airshell:

```
sudo airsh
```

3. Check your connection status:

```
airsh>> status conductor
```

You'll see Disconnected mode is on and the interval it is set to automatically reconnect:

```
Connection status: Disconnected
Disconnected mode: on
Reconnect interval (minutes): 60
Airwall Device ID: C9234588172
```



Note: If Disconnected mode shows as off, your Airwall Server is not in Disconnected mode. For assistance troubleshooting your connection, see [I'm having trouble connecting](#) on page 31 or contact your Airwall secure network administrator.

4. Manually sync with the Conductor:

```
airsh>> conductor sync
```

Your Linux Airwall Server reconnects to the Conductor and updates any configuration or trust policy changes since the last sync, then disconnects again.

See also: [Linux Airwall Server Airshell commands](#) on page 309

Change My Conductor Preferences

Change your Conductor password, theme and other options from your Preferences page.

1. Log in to the Conductor with your existing password.
2. Select the profile icon
3. To see more options, select **Preferences**.
4. Scroll down to change your API access token, Alert email trigger level, or show or hide the Dashboard Setup progress bar. Some settings you can change directly. For others, you need to select **Edit Settings**.

Change my Conductor password

You may need to change the password you use to log in to the Conductor.

1. Log in to the Conductor with your existing password.
2. Select the profile icon , and then select **Preferences**.
3. Under **Preferences**, click **Edit Settings**.
4. Scroll down to **Change your password**, and enter your current password. Then enter and confirm your new password, or click **Generate** to generate a password and copy it to the clipboard.
5. Select **Update Settings**.

Be sure to save your new password in a secure place.

Show or Hide Conductor Setup progress

You can show or hide the Conductor **Setup progress** bar on the Dashboard in your user preferences.

1. Log in to the Conductor with your existing password.
2. Select the profile icon , and then select **Preferences**.
3. Scroll down to **Show progress on dashboard**, and toggle it on (circle to the right) or off (circle to the left).

For more information on the Conductor tutorials, see [Get Started using Conductor Help and Tutorials](#) on page 118.

I'm having trouble connecting

Here's help for issues connecting to an Airwall secure network.

My agent or server is in disconnected mode

Normally, Disconnected mode will not affect your ability to access resources on the Airwall secure network. If you are having issues, you can manually sync with the Conductor. See [Sync an Airwall Agent or Server in Disconnected Mode](#) on page 29.

Cannot connect to a website even though I'm authenticated.

If you can't connect to a website you should be able to connect to, try:

- Making sure the web URL starts with https://.
- Check that you have access to the Internet. If you don't, your administrator may need to configure a DNS server on their end for you to access the Internet.

My Windows Airwall Agent won't connect when multiple interfaces are active

This issue can be caused by a Windows default that doesn't allow multiple simultaneous active network interfaces, and prefers ethernet over cellular or WiFi.

To bypass the default and have Windows keep multiple interfaces open, you edit the `fMinimizeConnections` registry value:

1. Hold the Windows Key down and press the R key.
2. In the **Run** dialog, type `regedit` and click **OK**.
3. Navigate to the following path in Registry Editor:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc`
4. See if the `GroupPolicy` subkey exists.
 - If it exists, check that the `fMinimizeConnections` value is 0.
 - If it doesn't exist, create it: Highlight `WcmSvc`, right click on `WcmSvc`, and select **New**, then select **Key**. Name the new key `GroupPolicy`. Right-click `GroupPolicy` and select **New**, select **DWORD (32-bit)**, and then select **Create value**. Name the value `fMinimizeConnections` and click **OK**. Check that the value is 0 (for false).
5. Reboot and test to see if the connection works over all network interfaces.

Linux Airwall Server or macOS Airwall Agent interface selection

The Linux Airwall Server and macOS Airwall Agent implement an interface auto-selection method. When you first install the Airwall Agent or Server, Linux or macOS determines the default gateway of the host and uses the associated network interface.



Note: Auto-selection is per profile.

Troubleshooting

If your Linux Airwall Server or macOS Airwall Agent is reporting as *online*, but doesn't seem to be working, check that the correct network interface is selected in the profile. This can be done by modifying `hip.conf` in the associated profile directory.

Example - List details of the active profile:

```
sudo airctl profile details --active

root@ubuntu-system-files:~# airctl profile details <profile_name>
profile_dir: profile1
profile_name: myprofile
network: ens4
deviceID:
overlay_device_ip:
overlay_mask:
conductor: myconductor.example.com:8096
log_level: info
```

You can find the settings for the active profile in the **profile1** folder under `/opt/tnw/profiles/profile1`. In that folder, open `hip.conf`, and change the `master_interface` key to the network interface you need.

Manage Airwall™

Monitor, Maintain, Provision, Control Access

The Conductor Dashboard

The Conductor Dashboard gives you a quick view into the health and state of your Airwall secure network, showing you activity and alerting across the entire network.

With the Dashboard, you can, depending on your permissions:

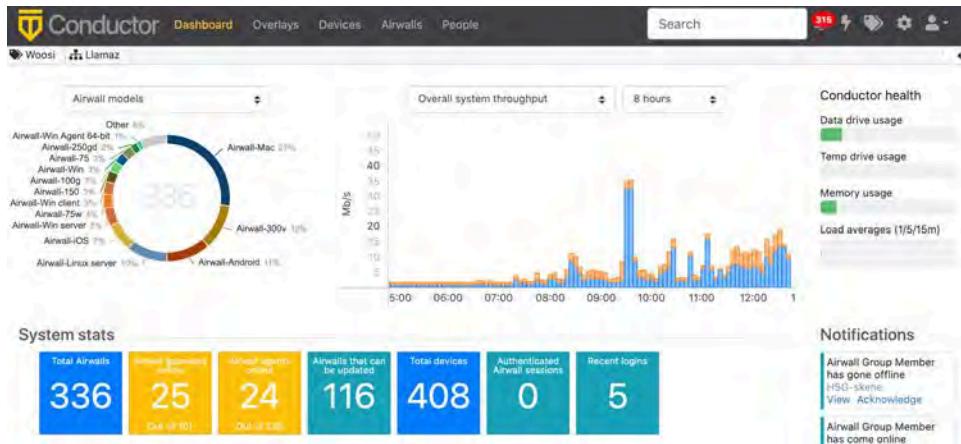
- See the state of the overlay networks that make up your Airwall secure network.
- See activity without needing management rights.
- Manage Airwall Edge Services and troubleshoot connection issues.
- Monitor the health of your network
- See at a glance changes within the system.

View network status

See the models and versions of Airwall Edge Services, and the overall system throughput for up to the last 24 hours.

The System stats are tiles that show at a glance how many Airwall Gateways and Airwall Agents and Servers are online, how many can be updated, and other useful information.

Click a stat tile to show more details in the Navigation pane below. For example, click **Airwall agents online** to see a list of the Airwall Agents and Servers that are online below.



Pin pages and Recently Viewed lists for quick access

Right under the menu bar, you'll now find a pin bar, where you can pin up to 20 pages you visit frequently to quickly get back to them. You can click the arrow on the right to see and pin **Recently viewed** items. On most pages, you can also click the pin icon to add the page to your pin bar. Click it again to remove the pin.



Note: To pin a device, open the device page, and then go to recently-viewed items to pin.



Navigation – System

The System navigation screen shows Messages from admins and firmware updates from Tempered, as well as recent events, such as provisioning requests and firmware updates. You can also see or create messages for other Conductor or network admins.

- To create a message, select the pencil icon. For more details, see [Create or Manage Dashboard Messages](#) on page 39.
- Under **Recent events**, select **View** on items to jump right to the page, or select **Manage** to manage and name without leaving the dashboard.

Navigation sidebar:

- System
- Airwalls
- Overlays
- Devices

Messages section:

- Fun fact: Kibbles started on 2.0.0 in 2017 and has been upgraded 180 times and counting! (Posted by Marshall at 06/17/2020 12:25:05 pm)
- Welcome to the Conductor! Enjoy your stay. (Posted by System at 03/31/2020 12:23:01 pm)

Recent events section:

Event Type	ID	Description	Action
New provisioning request	564D499189D3	Airwall-300v	View
New firmware available	Stay up-to-date!		View
New provisioning request	07C09B855697	ip-172-31-20-93 / Airwall-Linux	View
New Airwall online	B7E3B099CF1C	Airwall-300v	View Manage
New provisioning request	E3923C378E8A	WinDry1809Eval / Airwall-WiFi	View
New Airwall online	31E1FD097A36A	Airwall-300v	View Manage
New Airwall online	26A83DAE532	Airwall-300v	View Manage
New Airwall online	A8C4956F44FB	Airwall-Linux server	View Manage
New Airwall online	B3C40B068CE	Airwall-Linux server	View Manage

Navigation – Airwalls

Here's what you can do on the **Airwalls** navigation page:

- Select an Airwall Edge Service name to open it.
- Click one of the Airwall **System stats** tiles to see the details.



- Filter which Airwall Edge Services you see:
 - In the **Show all Airwalls** box, select an Airwall status (such as offline or unmanaged) to view.
 - Type in the **Filter** box to filter on name or model, or other aspects of the Airwall Edge Services, like Tags.

Airwall™ edge services			
		Show all Airwalls	Filter
		Items 1-25 of 336	
< > Sort by Name Page 1 of 14			
Airwall ▾		Model	Status
0-relay-AWS Airwall relay BH@40130#EC29D3655A06		Airwall-300v v2.2.8	● 52.32.158.3
0-relay-Orlie Airwall relay BH@40130#400020200002		Airwall-400 v2.2.8	● 216.168.34.211
009624AEFD5F BH@40130#009624AEFD5F		WindowsHPserver v2.2.3	○ 192.168.12.129
011D91958719 BH@40130#011D91958719		Airwall-Win server v2.2.0	○ 172.16.25.51
013E40F2DC5B BH@40130#013E40F2DC5B		Airwall-Android v2.1.2	○ 10.10.3.48
0432447A6A97 (unmanaged) BH@40130#0432447A6A97		Airwall-300v v2.2.2	○ 10.0.2.5
053D8ECAAF3B BH@40130#053D8ECAAF3B		Airwall-Android v2.1.5	○ 10.10.102.29
0D2EB919CBB1 BH@40130#0D2EB919CBB1		Airwall-Android v2.1.5	○ 10.10.24.89
		Airwall-Mac	○ 192.168.1.8

Navigation – Overlays

Here's what you can do on the Overlays navigation page:

- Select **New** to create a new Overlay. For more details, see [Create an overlay network](#) on page 355.
- Type in the **Filter** box to filter by **Name**.
- Select the drop-down menu to edit, tag, or disable the Overlay.
- Select an Overlay name to open it.

The screenshot shows the 'Overlays' section of the navigation interface. On the left, there's a sidebar with icons for System, Airwalls, Overlays (selected), and Devices. The main area has a title 'Overlays' with a 'Sort by Name' dropdown set to 'Name'. Below is a table with 27 items, showing names like '0-cameras', '0-hello-core-services', and various network-related overlays. A 'Filter' input field is at the top right, and a URL bar at the bottom contains 'https://kibbles.temperednetworks.com/app/#'.

Navigation – Devices

Here's what you can do on the **Devices** navigation page:

- Select a device to go to that device.
- Click the **Total Devices System stats** tile to open the **Devices** navigation page.



- Filter which **Devices** you see:
 - Select the **Sort by** box to sort the devices.
 - Type in the **Filter** box to filter by **Device name** or **Overlay IP**, among other things.

The screenshot shows the 'Devices' section of the navigation interface. The sidebar includes icons for System, Airwalls, Overlays, and Devices (selected). The main area has a title 'Devices' with a 'Sort by Name' dropdown set to 'Device name'. Below is a table with 408 items, showing device names like 'Internet', '009624AEFD5F', and IP addresses like '0.0.0.0/0' and '::/0'. A 'Filter' input field is at the top right, and a URL bar at the bottom contains 'https://kibbles.temperednetworks.com/app/#'.

Navigation – Provisioning

The **Provisioning** page gives you a quick way to see what Airwall Edge Services need to be managed and quickly handle these provisioning requests. You can:

- Select one or more Airwall Edge Services and grant or deny the provisioning requests. Check next to the Airwall Edge Services, then from the **Actions** menu, select **Grant request** or **Deny request**.
- Filter which Airwall Edge Services you see:
 - Sort the Airwall Edge Services by any column by clicking on the column .
 - Type in the **Filter** box to filter by **Model** or **Identifier**, or other things.

Navigation		Provisioning requests			
		Model	Identifier	Time	Status
System		Airwall-Linux	localhost:8B50CA70ECEA	05/22/2021 12:18:04 PM	Provisioning requested
Overlays		Airwall-300v	EC2D109BD40A	05/06/2021 12:25:35 PM	Provisioning requested
		Airwall-Linux	docker-desktop:0ADDCA452996	04/30/2021 2:56:21 PM	Provisioning requested
Devices		Airwall-Linux	docker-desktop:35D5E21C6D6E	04/30/2021 12:58:00 PM	Provisioning requested
Airwalls		Airwall-Linux	docker-desktop:5E86958170DB	04/30/2021 12:30:38 PM	Provisioning requested
Provisioning		Airwall-Linux	Router:2332C84AD8EB	04/28/2021 5:02:18 PM	Provisioning requested
		Airwall-Linux	Router:6D21DB7A24F4	04/28/2021 3:16:19 PM	Provisioning requested
		Airwall-300v	EC28B6BF3431	03/18/2021 4:16:22 PM	Provisioning requested
		Airwall-300v	4FD40267DA63	03/10/2021 9:57:20 AM	Provisioning requested
		Airwall-300v	EC2125C1CB04	03/08/2021 6:14:35 PM	Provisioning requested

Conductor Icon Reference

A reference for the icons you'll see used in the Conductor.

Type	Icon	Meaning
Common		
		Refresh
		Edit
		Delete
		Click to Pin to top bar, Pinned to top bar. Click to unpin.
Dashboard		
		Bypass destination
		System
		Airwalls
		Overlays
		Devices
People		
		People group

	Authenticated user
	Has an unused activation code. If grayed out, activation code has expired.
	People statuses
	Last 24 hrs
	Last week
	Longer than a week
	Never
Agents & Servers	
	Android Airwall Agent
	macOS or iOS Airwall Agent
	Windows Airwall Agent
	Airwall server
Overlays	
	Disable network communications disabled
	Enable network communications
	Enable transparent mode
	Enable protected mode
	Device statuses (on Overlay page)
Airwalls	
	Airwall
	Cloud Airwall - the overlaid icon indicates which type. In this case, AWS (Amazon Web Services).
	Airwall or Device group

		Ethernet Airwall
		Cellular Airwall
		Wifi Airwall
		Unmanaged
		Not authenticated
		Offline
		Revoked
		Icons superimposed on other icons to indicate which type of server, virtual, or cloud Airwall: Rackspace, VMware, Openstack, AWS, Azure, HyperV, Xen, Google, Alibaba Cloud
		Mac Lockdown
Devices and Device Groups		
		Device
		Discovered device (not yet accepted)
		Device or Airwall group
		Smart device group
		Recompute disabled on this Smart Device Group, and there are devices that would be in this group. Click the action menu to recompute the devices added using the rules.
Alerts and monitoring		
		Disabled on alert line
		Disabled on menu
		Alerts
		Event Monitors
		Tags



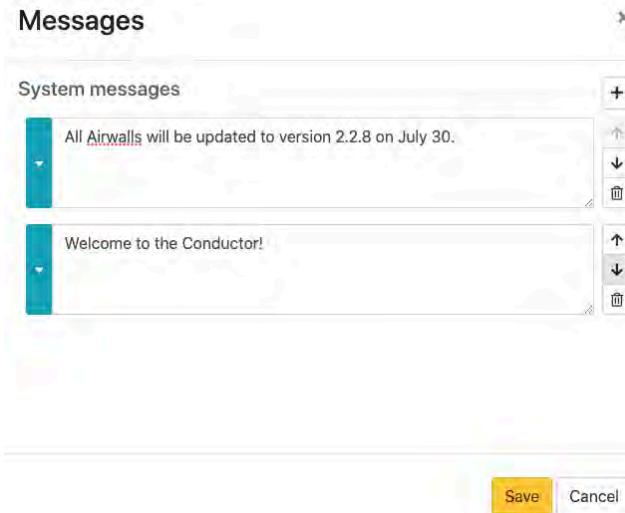
Create or Manage Dashboard Messages

Create messages that appear on the Conductor Dashboard to notify other administrators about upcoming firmware updates or other events that other administrators need to know about.

1. On the Conductor Dashboard, scroll down to the Navigation section, and open the System pane.
2. Select the pencil icon in the upper right of the pane to create or manage messages.
3. In Messages, to create a new message, select the + and write your message.
4. Select the color drop-down on the left to select the color of the message bar. Your organization can decide how to classify messages. Here is a starting point:
 - Blue: Informational messages
 - Green: Resolved or managed events
 - Yellow: Warnings about non-blocking system issues
 - Red: Blocking system issues, downtime, or outages

The screenshot shows the 'Messages' section of the Conductor Dashboard. It displays a list of system messages with a color-coded bar on the left. The first message, 'All Airwalls will be updated to version 2.2.8 on July 30.', is highlighted. Below the list are four colored bars: blue, green, yellow, and red. At the bottom of the interface are 'Save' and 'Cancel' buttons.

5. Use the side arrows or trash can to reorder or remove existing messages, as needed. If you don't rearrange them, messages are displayed with the latest messages at the top.



6. Select Save.

Change My Conductor Preferences

Change your Conductor password, theme and other options from your Preferences page.

1. Log in to the Conductor with your existing password.
2. Select the profile icon .
3. To see more options, select **Preferences**.
4. Scroll down to change your API access token, Alert email trigger level, or show or hide the Dashboard Setup progress bar. Some settings you can change directly. For others, you need to select **Edit Settings**.

Change my Conductor password

You may need to change the password you use to log in to the Conductor.

1. Log in to the Conductor with your existing password.
2. Select the profile icon , and then select **Preferences**.
3. Under **Preferences**, click **Edit Settings**.
4. Scroll down to **Change your password**, and enter your current password. Then enter and confirm your new password, or click **Generate** to generate a password and copy it to the clipboard.
5. Select **Update Settings**.

Be sure to save your new password in a secure place.

Show or Hide Conductor Setup progress

You can show or hide the Conductor **Setup progress** bar on the Dashboard in your user preferences.

1. Log in to the Conductor with your existing password.
2. Select the profile icon , and then select **Preferences**.
3. Scroll down to **Show progress on dashboard**, and toggle it on (circle to the right) or off (circle to the left).

For more information on the Conductor tutorials, see [Get Started using Conductor Help and Tutorials](#) on page 118.

Customize the Conductor

You can customize the Conductor login screen and emails sent from the Conductor for your business.

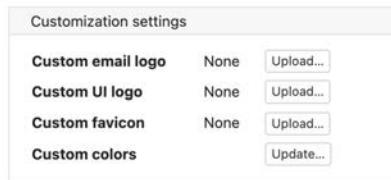
Here's what you can customize:

- **Conductor** login screen – Add your company logo, and change the background colors and favicon.
- **Conductor emails** – Add your company logo and change the text color. You can also customize the subject line and add a note from the administrator when sending Airwall Invitations.

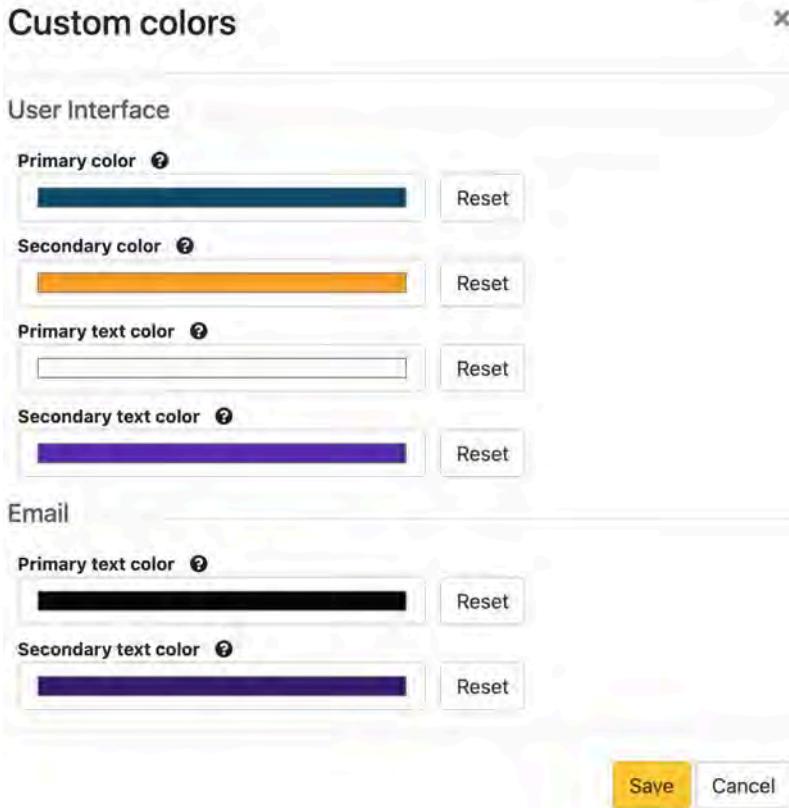
Keep reading for more details and examples.

Customize the Conductor Login page

1. Go to **Settings > Customization settings**.



2. Under **Custom UI logo**, select **Upload**, select **Choose File**, and choose the logo you'd like to appear on the login page, then select **Upload**.
3. Under **Custom favicon**, select **Upload**, select **Choose File**, and choose the favicon you'd like to appear on your web browser tab, and then select **Upload**.
4. Under **Custom colors**, select **Update**, and under User Interface, select the colors you'd like to use on the Conductor login page, and then select **Save**.

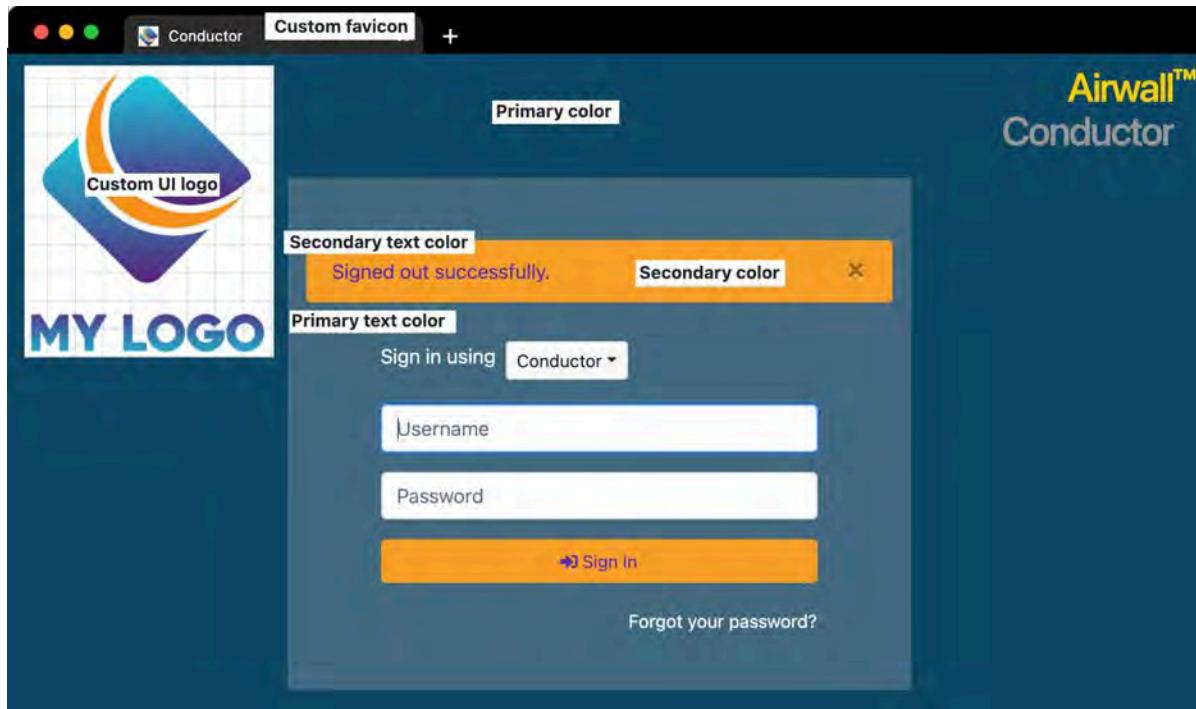


5. Refresh your browser window to see the favicon change. Log out to see your login page changes.

Now the Conductor login page will use your customizations.

Example

Here is an example of what the Conductor login page looks like with a custom logo, favicon, and colors, showing how your selections will map to the page:



Customize Conductor emails

Customize the emails sent by the Conductor to reflect your company's branding.

Before you Begin

Before you can customize the emails, you need to:

- Set up your email settings in the Conductor. To do this, see [Configure Email Settings](#) on page 200.
- Make sure the size of the logo and icon files you want to use are 10MB or less.

Customize emails

1. Go to **Settings > Customization settings**.

Customization settings			
Custom email logo	None	<input type="button" value="Upload..."/>	
Custom UI logo	None	<input type="button" value="Upload..."/>	
Custom favicon	None	<input type="button" value="Upload..."/>	
Custom colors		<input type="button" value="Update..."/>	



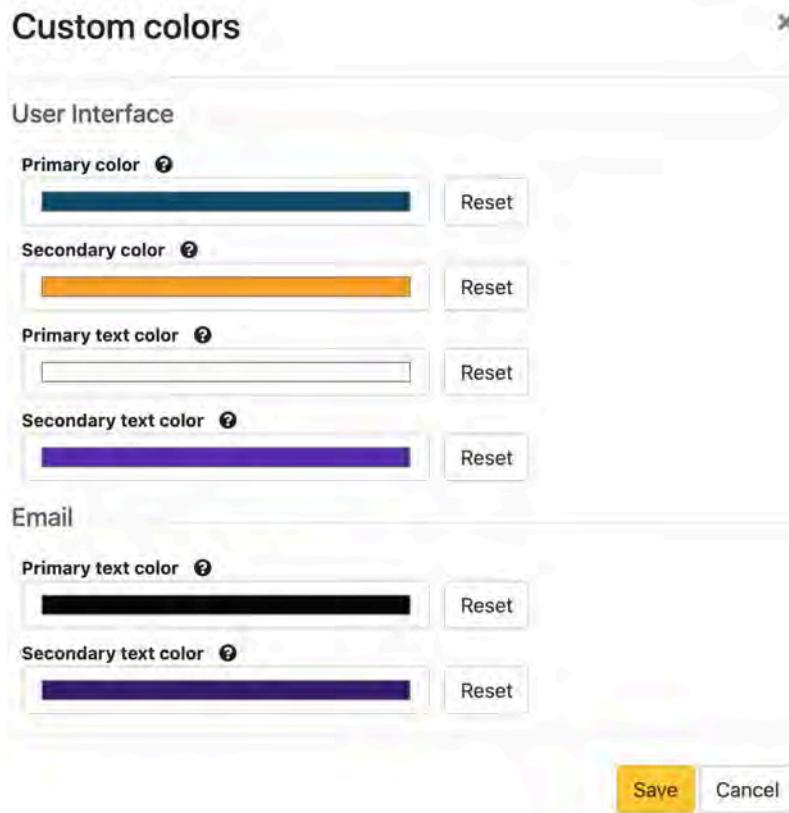
Note: If you can't see all of these options, make sure you've set up your email settings in the Conductor. See [Configure Email Settings](#) on page 200.

2. Next to **Custom email logo**, select **Upload**, select **Choose File**, and choose the logo you'd like to appear in emails from the Conductor, and then select **Upload**.



Tip: Allowed image types are .png, .jpg, .jpeg, and recommended sizes are, in pixels: 200x60, 400x120, 800x240, 1600x480.

3. Next to **Custom colors**, select **Update**, and under **Email**, select the primary and secondary text colors you'd like to use in emails from the Conductor, and then select **Save**.

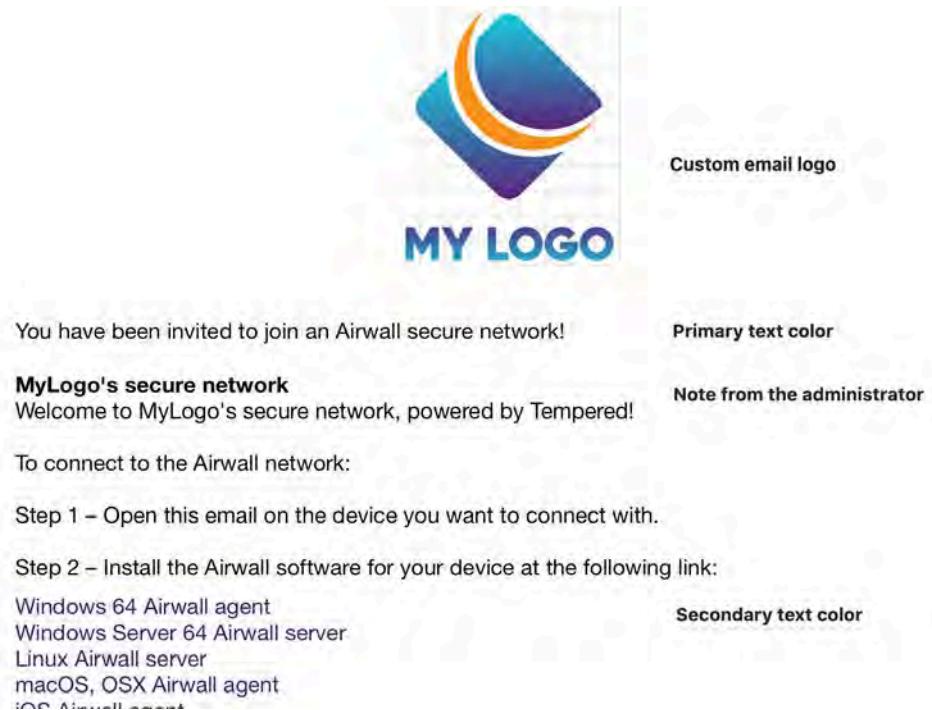


4. When you create Airwall Invitations, you can also customize the subject of the email and add a note from the administrator to the top of the email. For more information, see [Connect People's Devices with Airwall Invitations](#) on page 54.

Now all emails you send from the Conductor will use your customizations.

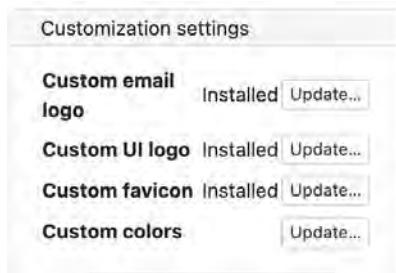
Example

Here is an example of what emails from the Conductor look like with a custom logo and custom text colors, showing how your selections will map to the emails:



Remove Conductor customizations

1. Go to **Settings > Customization settings**.



2. To reset logos and favicons – Next to **Custom email logo**, **Custom UI logo**, and **Custom favicon**, select **Update**, and then select **Remove**.
3. To reset colors – Next to **Custom colors**, select **Update**, and then select **Reset** for any color you'd like to remove.
4. Refresh the browser window to see your changes.

Manage People

Manage Conductor admins and people connecting to your Airwall secure network with laptops and mobile devices.

Manage Conductor Admins

Create accounts and people groups in the Conductor to manage the administrators who access your Airwall Conductor and your overlay networks and devices.

Add a Person

Add a person and give them a role that determines what they can access on the Conductor and/or your Airwall secure network.



Note: If you are onboarding people using LDAP or a third-party authentication provider, people are imported as they log in. See [Configure LDAP authentication on Conductor and Airwall Edge Services](#) on page 219 and [Configure LDAP to manage user roles](#) on page 227, or [Integrate Third-party Authentication with OpenID Connect](#) on page 208.

1. Log in to the Conductor with a system administrator account and go to **People**.
2. On the **People** tab, select **New Person**.
3. Under **Status**, select whether to create this account as **Active** or **Inactive**. You can use this option to set up people's accounts prior to onboarding, or to deactivate a person's account as needed.
4. Under **User directory**, usually you leave it at **Local User List**, providing authentication through the Conductor. See note above if you are using LDAP or a third-party authentication provider.
5. Enter the person's information: **Username** and **Email** are required.
6. Under **Role**, select the Conductor role for the person.

For more information on:

- Conductor roles – See [Understand People Roles and Permissions](#) on page 49.
- Custom permissions for System and Network Administrators – See [Customize Permissions for System and Network Administrators](#) on page 46

7. (Optional) If you give the person an administrator role, select their initial **Alert email trigger level**.



Note: Administrator roles can log in and change their alert level.

8. For password, you have two options:
 - **User sets their own password** – Select **Send new user an email with a link to set their password** to let the user set their own password.
 - Or, **Set a password for the user** – Select **Set a password for the user to log in**. You can either enter a password, or select **Generate** to generate a password and copy it to your clipboard.



Note: If you choose to set the password, you need to provide the username and password you created to the person.

9. Click **Create person**.



Note: New accounts are active by default. A person can log in with the account after a few minutes. To create a user as inactive, or change their status to Inactive, under **Status**, select **Inactive**.

Once you've created the person's account, you can add them to **People groups** or Overlay networks.

The screenshot shows the Conductor interface with the title "People - Local Administrator". The left sidebar lists account details: Local Administrator Account, User directory (Local Accounts), Full name (Local Administrator), Username (admin), Role (System Administrator), Status (Active), API access (Disabled), Email (global-admin@temperednetworks.com), and Phone. The right side shows sections for "Info" (Edit settings, No tags in use), "People groups" (Edit..., Not a member of any people groups), and "Overlay networks" (Edit..., Not a member of any overlay networks). The top navigation bar includes Dashboard, Overlays, Devices, Airwalls, People, Search, and a notification badge for 102 items.

Related tasks

[Set up a People Group](#) on page 74

Set up a people group to make it easier to manage the people accessing your secure network.

[Edit members of an overlay network](#) on page 356

Overlay networks can only be modified by users who are managers of that network. After creating an overlay network, you may want to add additional managers to your overlay network or edit their roles.

Change a Person's Account

Edit a person's account to change how they access the Conductor. You can edit settings such as whether the account is active or inactive, change passwords, change roles, and more.

1. Log in to the Conductor with a system administrator account and click **People**.
2. Select a person to open their page. You can sort or filter the list of people to find the person you're looking for.
3. Select **Edit Settings**.
4. Make the changes to the account.

For more information on:

- Conductor roles – See [Understand People Roles and Permissions](#) on page 49.
- Custom permissions – See [Customize Permissions for System and Network Administrators](#) on page 46

5. Select **Update Settings**.

Customize Permissions for System and Network Administrators

You can fine-tune the permissions for System and Network administrators in your Airwall secure network.

System and Network administrators have a set of permissions by default in the Conductor. You can customize what these permissions are by default, and you can customize the permissions for individual system and network administrators.

Roles

System Administrators with **Can edit user permissions** enabled.

Customize Default Role Permissions

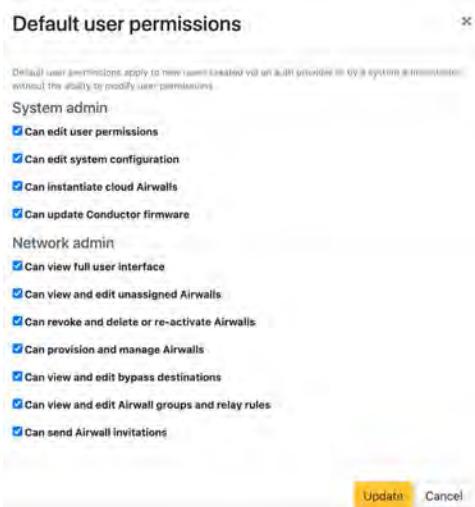
You can set the default permissions that are given to people who are newly assigned the system and network administrator roles in the Conductor.



Note: Default user permissions apply only to people currently being added to a role (both new users and users who are changing roles). It does not change the permissions of people already assigned that role. The defaults can be modified as a user is created if the person making the change has "Can edit user permissions" permission.

1. Go to **Settings > Authentication**.
2. Under **Default user permissions**, select **Edit Settings**.

- Check the permissions you want new people to have by default when they are assigned these roles.



- Select **Update** to save.

Customize Permissions for individual System and Network Administrators

If you are a system administrator with **Can edit user permissions** active, you can customize the permissions for system and network administrators.

- Go to **People**, select a person to open their page, and then select **Edit Settings**.
- Under **User permissions**, check or clear the permissions you want this person to have.

System Administrator customizable permissions

Details		User permissions
Status	Active	<input checked="" type="checkbox"/> Can edit user permissions
Full name	Joe Banks	<input checked="" type="checkbox"/> Can edit system configuration
Username	jbanks	<input checked="" type="checkbox"/> Can update Conductor firmware
		<input checked="" type="checkbox"/> Can instantiate cloud Airwalls

Network Administrator customizable permissions

User permissions
<input checked="" type="checkbox"/> Can view full user interface
<input checked="" type="checkbox"/> Can view and edit unassigned Airwalls
<input checked="" type="checkbox"/> Can revoke and delete or re-activate Airwalls
<input type="checkbox"/> Can provision and manage Airwalls
<input type="checkbox"/> Can view and edit bypass destinations
<input checked="" type="checkbox"/> Can view and edit Airwall groups and relay rules
<input type="checkbox"/> Can send Airwall invitations

For more information about these permissions, see [Customizable Permissions Descriptions](#) on page 48.

- Select **Update Settings**.

Customizable Permissions Descriptions

These are the permissions that can be customized for people assigned the System or Network Administrator roles.

Permission	Description
For System Administrators:	
Can edit user permissions	Can edit Conductor default permissions and permissions for individual users, including assigning user roles and customizing their permissions. Can also create new overlay networks and assign them to a network admin to manage trust.
Can edit system configuration	Administrator can edit Conductor Settings, including High Availability (HA), email server, remote logging, authentication, or any other settings in Settings > General .
Can create and configure cloud features	Can create and configure cloud Airwall Gateways, and create an HA-paired Conductor in the cloud.
Can update Conductor firmware	This option is available if you have checked Can edit system configuration . Can update the Conductor software and Airwall Edge Service firmware from Settings > Firmware updates
For Network Administrators:	
Can view full user interface	When clear, the user sees a simplified, easier-to-use view in the Conductor. For a description of the simplified view, see Set a Streamlined View for a Network Administrator on page 48.
Can view and edit unassigned Airwalls	Can view or edit any Airwall Edge Services that are not assigned to any overlay networks, including adding the devices in these Airwall Edge Services to any overlay networks they have permission to.
Can revoke and delete or re-activate Airwalls	Requires that Can view and edit unassigned Airwall is checked. Can revoke, delete, and re-activate Airwall Edge Services in their overlay networks, and can view and reactivate any revoked Airwall Edge Services.
Can provision and manage Airwalls	Requires that Can view and edit unassigned Airwall is checked. Can view and provision provisioning requests, and can manage unmanaged Airwall Edge Services.
Can view and edit bypass destinations	Can view and edit any bypass destinations.
Can view and edit Airwall groups and relay rules	Can view and edit Airwall groups and relay rules for Airwall Edge Services in their overlay networks.
Can send Airwall Invitations	Can send Airwall Invitations to invite users to connect to the Airwall secure network and gain access to the devices in their overlay networks.

Set a Streamlined View for a Network Administrator

When you set the permissions for a Network administrator, you can clear the **Can view full user interface** permission, which provides the Network administrator with a streamlined view that can simplify their workflow.

Network administrators using the streamlined view can manage their overlays, and the devices, Device groups, and Airwall Edge Services in them.

1. Go to **People**, and open the People page for the Network administrator.
2. Select **Edit Settings**.
3. Clear the **Can view full user interface** box.
4. **Update Settings**

The Network administrator now sees a streamlined view.



Note: You can also set the streamlined view as the default for all newly-assigned Network administrators. See [Customize Permissions for System and Network Administrators](#) on page 46.

To see what Network administrators with a limited view can see, see [Manage Overlay Networks in Streamlined View](#) on page 97.

Understand People Roles and Permissions

When you add a person to the Conductor, the person's role, and whether the person is a manager or member of an overlay, controls whether they have access to create, edit, or view overlay networks and their Airwall Edge Services and devices.

The Conductor supports the following people roles, with the following default permissions. You can also fine-tune permissions for System and Network Administrators. See [Customize Permissions for System and Network Administrators](#) on page 46:

- **System Administrator** - Designed for administrators who may need to perform all Conductor functions. By default, a system administrator can edit all Airwall Edge Services in the system and is a de facto editor of all Airwall Edge Services and overlay networks. Depending on granular user permissions, a system administrator can modify other users' permissions, edit system-level configuration (such as SMTP, Conductor HA pairing, remote syslog), create cloud Airwall Gateways, and upgrade the Conductor firmware.
- **Network Administrator** - Designed for administrators who need to manage and potentially modify existing overlay networks, Airwall Gateways and devices. Depending on granular user permissions, a network administrator can view and edit unassigned (not part of an overlay network) Airwall Edge Services, revoke and delete Airwall Edge Services, and provision and manage Airwall Edge Services. A network administrator cannot create new users or overlay networks or edit system configuration.
- **Read-only System Administrator** - Designed for administrators who need to monitor overlay networks, Airwall Gateways, and device information, but who do not have a need to modify configurations. A read-only system administrator can view all Airwall Edge Services in the system and is a de facto viewer of all overlay networks. A read-only system administrator can also run reports and perform diagnostic functions on the Conductor and Airwall Edge Services.
- **Remote Access User** - This role is for people who need access to an Airwall secure network through an Airwall Agent or Server. This user can only modify their account email and password. Remote access users can also view the remote access portal where they can see any activation codes assigned to them, a list of remote devices they have access to, and a list of the Airwall Edge Services assigned to them.

This table shows the default permissions. To customize these permissions, see [Customize Permissions for System and Network Administrators](#) on page 46

Task	System Administrator	Network Administrator	Read-only System Administrator	Remote Access User
Manage users	Create Modify Delete	Modify own email and password	View all users. Modify own email and password	Modify own email and password
Manage Conductor settings	Configure (with permissions)	Not available	View	Not available
Manage overlay networks	Create Modify Delete	View Modify	View	Not available

Task	System Administrator	Network Administrator	Read-only System Administrator	Remote Access User
Manage Airwall Edge Services	Add Modify Delete	Add (with permissions) Modify Delete	View	Not available
Manage devices	Add Modify Delete	Add Modify Delete	View	Not available
Manage firmware updates	Download Update Publish	Update	Not available	Not available

See Also:

- To customize permissions, see [Customize Permissions for System and Network Administrators](#) on page 46
- For pre-3.0 roles, see [Understand People Roles \(v2.2.13 and earlier\)](#) on page 50

Understand People Roles (v2.2.13 and earlier)

When you add a person to the Conductor, the person's role, and whether the person is a manager or member of an overlay, controls whether they have access to create, view, or edit overlay networks and their Airwall Edge Services and devices.

The Conductor supports the following people roles:

- System Administrator - Designed for administrators who need to perform all Conductor functions. A system administrator can edit all Airwall Edge Services in the system and is a de facto editor of all overlay networks. Depending on granular user permissions, a system administrator can modify other users' permissions, edit system-level configuration (such as SMTP, Conductor HA pairing, remote syslog), create cloud Airwall Gateways, and upgrade the Conductor firmware.
- Network Administrator - Designed for administrators who need to manage and potentially modify existing overlay networks, Airwall Gateways and devices. Depending on granular user permissions, a network administrator can view and edit unassigned (not part of an overlay network) Airwall Edge Services, revoke and delete Airwall Edge Services, and provision and manage Airwall Edge Services. A network administrator cannot create new users or overlay networks or edit system configuration.
- Read-only System Administrator - Designed for administrators who need to monitor overlay networks, Airwall Gateways, and device information, but who do not have a need to modify configurations. A read-only system administrator can view all Airwall Edge Services in the system and is a de facto viewer of all overlay networks. A read-only system administrator can also run reports and perform diagnostic functions on the Conductor and Airwall Edge Services.
- Remote Access User - This role is for people who need access to an Airwall secure network through an Airwall Agent or Server. This user can only modify their account email and password. Remote access users can also view the remote access portal where they can see any activation coes assigned to them, a list of remote devices they have access to, and a list of the Airwall Agents and Servers assigned to them.

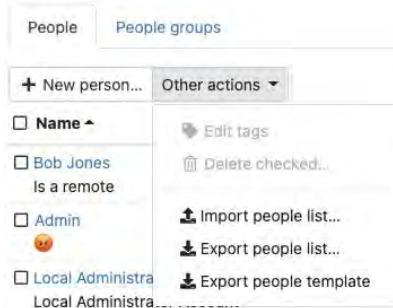
Task	System Administrator	Network Administrator	Read-only System Administrator	Remote Access User
Manage users	Create Modify Delete	Not available	View	Modify own email and password

Task	System Administrator	Network Administrator	Read-only System Administrator	Remote Access User
Manage Conductor settings	Configure	Not available	View	Not available
Manage overlay networks	Create Modify Delete	View Modify	View	List of Overlays they are in only
Manage Airwall Edge Services	Add Modify Delete	Add Modify Delete	View	Not available
Manage devices	Add Modify Delete	Add Modify Delete	View	Not available
Manage firmware updates	Download Update Publish	Update	Not available	Not available

Import people using a CSV file

You can add many local users to the Conductor at one time by importing them in bulk. You export a .csv file as a template or with current users, and then import to add people to the Conductor in one step.

1. In the Conductor, go to the **People** page.
2. Under **People**, open **Other actions..**.



3. Select **Export people list**, or **Export people template** and then confirm the export. You can use either to import people. The people list allows you to see and modify some options for people already in the Conductor.
4. Edit the .csv file that you downloaded to add people. See [Import People .csv File Details](#) on page 52 for an explanation of the columns. The minimum required columns are `username`, `role`, `name`, `email`, and `active`. Leave the password blank to send the person an email with a link to set their password. If you do include passwords, make sure they meet the password criteria. For information on setting password criteria, see [Configure Authentication Options](#) on page 203.

Note: For existing people in the .csv file, you can also modify roles, permissions, and most other options. You cannot change passwords or remove people using the .csv.

5. Back on the **People** page, open **Other actions** again.
6. Select **Import people list**, select **Choose File**, and then select the file you edited and select **Upload**.
7. If validation fails, correct the file and try again.

- Once the import passes validation, review the list of people being added, and select **Next** and then **Commit** to add them.

If you need to make any changes once the file is imported, you can edit the .csv and then re-import. It will modify the account for existing people (except for changing or removing passwords or removing people). After a person is added to the Conductor, you must manage passwords individually from each person's page.

Import People .csv File Details

The import people .csv has the following columns:

Column	Description	Example
username	<i>Required.</i> Enter a unique username. <i>Cannot update for existing users.</i>	joebanks
role	<i>Required.</i> Person's role in the Conductor. Must be one of: <ul style="list-style-type: none"> • system_admin • viewer • network_admin • remote_user 	remote_user
name	<i>Required.</i> Full name, with first name first.	Joe Banks
description	<i>Optional.</i> Description for the person.	Admin for Building 1
email	<i>Required.</i> A valid email for the person.	jbanks@tempered.io
phone1 and phone2 (both optional)	<i>Optional.</i> Phone number for the person.	+12065551212
active	<i>Required.</i> Add the person as an active user. Boolean TRUE or FALSE. In most cases, you want to have this as TRUE.	TRUE
password	<i>Optional.</i> If you want to set a password for the user, you can enter it here. If you have SMTP set up on your Conductor, you can leave it empty, the Conductor sends an email to the new user asking them to log in and set their password. <i>Cannot update for existing users.</i>	very_secure_P@assword

Column	Description	Example
api_user	<i>Optional.</i> Add the person with rights to use the API. Boolean TRUE or FALSE. Only available for system_admin, network_admin, and viewer roles.	TRUE
email_alert_level	<i>Optional.</i> Enter the Conductor alerts this person should get in email. Must be one of: <ul style="list-style-type: none"> • none • info • warning • error 	none
tags	<i>Optional.</i> Apply existing or new tags to people, in the format [“tag1”,“tag2”]. To make no changes, leave blank. To remove all tags, enter an empty array []. See Template Note .	["fte", "engr"]
person_groups	<i>Optional.</i> Apply existing or a new set of people groups to people, in the format [“person group name 1”, “person group name 2”]. To make no changes, leave blank. To remove the person from all people groups, enter an empty array []. See Template Note .	["building 2", "2nd floor"]

Template Note: The first row on the people_template.csv that you download has empty arrays for the tags and person_groups columns. These empty arrays will remove the tags and person_groups if you enter an existing person on that line.

When you import your .csv file, the Conductor validates the file and warns you of any detected issues. Edit the .csv to fix any issues and re-import. Once it validates, you can select Commit and the Conductor adds and updates the people on your list.

Remove people in bulk

You can delete users in bulk from the **People** page.

1. In the Conductor, go to the **People** page.
2. Select the people you want to delete.
3. Under **People**, open **Other actions**.
4. Select **Delete checked**.
5. Confirm the list of people to delete, and select **Delete**.

Connect People's Devices to your Airwall secure network

How to connect cell phones, laptops, and servers to the resources people need access to behind your Airwall secure network.

People connect their devices to your secure network using Airwall software installed on their devices, called Airwall Agents and Servers. There are Airwall Agent or Server software applications for the most common device types.

The easiest way to get your users started is to [Set up a People Group](#) on page 74 and send people an Airwall Invitation or Activation code. You can also [Connect People as Remote Access Users](#) on page 61. Using these methods automates much of the process for both the people connection and for you, the Conductor administrator.

Here's how it works:

1. For people who need to connect their devices to your Airwall secure network, you send them **Airwall Invitations** or Activation Codes. You can send a single invitation or send in bulk, and can choose whether to invite by email or by downloading activation codes to distribute yourself.
2. For the people you've invited:
 - Via email **Airwall Invitations**, they open the invitation email and click the link.
 - Via activation codes, they open the link to go to the **Connect an Airwall Agent** activation page.
3. They download and install an Airwall Agent or Server onto their device.
4. Once the Airwall Agent or Server is installed, they click the link in the email or **Connect an Airwall Agent** page to activate their account.
5. Once a person activates their account, the Conductor automatically takes care of all the steps to provision, license, manage, and name the new Airwall Agents and Servers.

You can send **Airwall Invitations** or Activation codes in bulk to entire organizations, and manage the connections and what they have access to in the Conductor.

Help for your users to install the software and connect is here: [Connect to Airwall](#) on page 6.

If you choose not to use **Airwall Invitations** or Activation codes, the people connecting need to download and install the software, and then enter the Conductor address manually. You then need to review the provisioning requests, confirm device IDs with each person, and grant access to each person's Airwall Agent or Server.

If you need to install the software from the Conductor, see [Install Airwall Agents and Servers on people's laptops and devices](#) on page 290.

Connect People's Devices with Airwall Invitations

Airwall Invitations greatly simplify the steps required to add people's mobile phones, tablets, and computers to your Airwall secure network.



Note: Another way to automate the process is using Activation Codes or adding people as Remote Access Users and adding them to a people group. See [Connect People's Devices with Activation Codes](#) on page 63, or [Connect People as Remote Access Users](#) on page 61 and [Set up a People Group](#) on page 74.

The [Walkthrough -- Send Expiring Guest Access Invitations](#) on page 57 provides an example or how to set up **Airwall Invitations** that you can modify to meet your organization needs.

Send Airwall Invitations

You send **Airwall Invitations** to invite people to connect to your Airwall secure network. It can be as simple as sending the invitations to a list of email addresses. With a bit of preparation, though, you can also automatically set up device access and trust as people connect their devices.

The possibilities include setting up which Overlay networks people belong to, what groups they're a part of, which Airwall Edge Services and devices they can access, and when a person's access to your Airwall secure network expires.

Before you begin

- Gather email lists for the types of people you need to grant access to

- (Optional) Group emails by people who need the same access permissions.
- (Optional) Create **Airwall groups** for the people you want to add. For example, you may want Employees and Contractors Airwall groups.
- (Optional) Create tags for the types of people and access.
- (Optional) Create Smart Device Groups to automatically add people to Device groups as they activate their Airwall Agents and Servers.

By doing a bit more planning and preparation in the optional steps above, you'll save time in making sure people are able to access the resources they need. For a walkthrough showing how to set up invitations that automatically provide guests with access to your secure network for 4 hrs, see [Walkthrough -- Send Expiring Guest Access Invitations](#) on page 57

1. Go to **Airwalls > Airwall Invitations**.
2. *If you have already sent invitations*, you can open the drop down next to an invitation and select **Use as Template** to send a similar invitation to more people. **To create a new invitation**, click **New Airwall Invitations**.
3. In v3.0 and later, select how you want to invite people. Select each option to see a description.

Airwall Invitations

Airwall invitations allows users to easily configure and deploy Airwalls

- Give activation codes to existing users
 Send activation codes via email
 Download activation codes and distribute them manually
 Download a single activation code that can be used many times

Existing users will be given an activation code that is accessible from the remote access portal. The remote access portal contains instructions for downloading an Airwall agent or server and connecting to Conductor with a single click. Users will be sent an email with instructions for connecting to the remote access portal.

Users

No entries

<< Back >> Next Cancel

4. After you select how to invite users, you'll need to enter the options for that type. For example, enter users if inviting current users, or email addresses for the group of people you want to connect to your Airwall secure network.
5. Click **Next**.

6. Enter the options that are on the dialog for your invitation type. Setting these options automates more of the process for the people trying to connect:
 - a) **Profile name** – This is the name of the profile to create on the people's Airwall Agents and Servers.
 - b) **Conductor hostname or IP** – Sets the Conductor they connect to.
 - c) **Generated Airwall name** – Sets the name the Airwall Agent or Server has when the user activates it. The default value sets it to the email address followed by their Airwall Agent or Server type. See the help when you select this box to see other options for autogenerated names.
 - d) **Activation codes should expire** – Check or clear this box, and if checked, set the **Activation code expiration date** – Sets the date the Airwall Invitation expires.

Airwall Invitations

Configure settings for how to download, install and activate Airwalls

Profile name	optional	Dynamically name Airwall agents when they connect to the Conductor by enclosing them in \${field_name}.
Conductor hostname or IP	pogo2.temperednetworks.com	Available fields:
Generated Airwall name	<code>\$(email_name)'s \${airwall_type}</code>	<code>email</code> - Email address <code>email_name</code> - Email address without domain <code>full_name</code> - User's full name <code>hostname</code> - Hostname <code>airwall_type</code> - Installed Airwall type <code>ip</code> - Airwall agent's overlay device IP
Activation codes should expire	<input checked="" type="checkbox"/>	
Activation code expiration date	10/22/2021	

[**<< Back**](#) [**>> Next**](#) [**Cancel**](#)



Note: pre-2.2.8 Conductors also have: Install Package Location – Enter a place accessible to your invitees where you've downloaded the Airwall Agents and Servers software, or point to the latest version in Airwall help: https://webhelp.tempered.io/webhelp/content/topics/downloads_latest.html

7. Click **Next**.
8. Enter additional settings to automate people's access as their devices connect:
 - a) **Overlay device IP network (CIDR)** – (Optional) The network from which to assign IP addresses to devices as they connect.

Note: If you use the same IP network in subsequent Invitations, IP addresses will keep incrementing. For instance, if you send out one Invitation starting at 192.168.1.15 with 10 emails and then another with the same IP with 10 emails, they all just get a free IP from the network as they come online.
 - b) **Overlay networks** – (Optional) The overlay networks to add people's devices to.
 - c) **Device groups** – Select the **Device groups** to add devices to.
 - d) **Airwall groups** – Select **Airwall groups** to add Airwall Agents and Servers to. For example, you might assign these Airwall Agents and Servers to the Employee, Admin, or Vendor group.
 - e) **Tags** – Create or assign tags to people's devices. For example, if you're using tags to create Smart Device Groups that add people's devices to the right overlays, enter these tags now.
9. If you are generating Activation codes, select **Generate** and skip the rest of these steps.
10. If you are inviting existing users or sending emails, select **Next**.

11. Double-check the email addresses and make any needed changes to the invitation email. To help the people receiving Activation codes to connect, point them to one of these help topics: [I have an Airwall Invitation](#) on page 13 or [I have an Activation Code](#) on page 14.
12. Click **Finish** to send the invitations.

Resend an Invitation

If you've sent an invitation and the person hasn't received it, or their invitation has expired before they activated it, you can resend it by using the original invitation as a template to create a new invitation. See [Reuse an Invitation](#) on page 57 to send a new invitation with a new expiration date.

Disable an Invitation

If you've sent an invitation and no longer want the person to be able to activate it, you can disable it.

1. In your Conductor, go to the **Airwalls** page.
2. Open the **Airwall Invitations** tab and find the invitation you want to disable.
3. Open the dropdown on the far right of the invitation row and select **Disable Invitation**.

Reuse an Invitation

If you have already created an invitation with the options needed for a new invitation, you can easily reuse it. Some of the information for the invitation will be already filled in.

1. In your Conductor, go to the **Airwalls** page.
2. Open the **Airwall Invitations** tab and find the invitation you want to disable.
3. Open the dropdown to the far right of the invitation row and select **Use as Template**.
4. Click through and fill in the information needed and click **Finish** to send.

Walkthrough -- Send Expiring Guest Access Invitations

In this walkthrough, you set up and send **Airwall Invitations** that provide guests with 4 hours of access to your Airwall secure network, after which it automatically disables all communications.

One way you can use **Airwall Invitations** to group and configure people's devices as they accept the **Airwall Invitations** and connect to your Airwall secure network is to expire people's access to your secure network at a time you set.

Setting access that expires is useful when you have people, such as vendors or guests, that you want to give access to, but you want to enforce a time limit automatically.

You can modify this walkthrough to create your own rules for automatically configuring Airwall Agents and Servers using **Airwall Invitations**.

Walkthrough Overview

To create Airwall Invitations that expire, you need to:

1. **Create two Tags** – One to grant access and one to remove access. For example, if you're creating guest access, you might create tags of `Guest Access4hr` and `Guest Disabled`.
2. **Create two Smart Device Groups** –
 - a) **Grant Access Group** – Create a rule that adds devices to the group if they have the `grant access` tag you created. For example, you might create a Smart Device Group called `Guest Access` and create a rule that adds devices tagged with `Guest Access4hr`.
 - b) **Remove Access Group** – Create a rule that adds devices to the group if they have the `remove access` tag you created. For example, you might create a Smart Device Group called `Disabled Guests` with a rule to add devices tagged with `Guest Disabled`.
3. **Add the Grant Access group to the appropriate Overlays** – Add the Grant Access group to the Overlays that give the people's devices access to the resources they need.



Note: Do NOT assign the Remove Access Device Group to any Overlay Network. This Device Group is added as a negative to any other Smart Device Groups to prevent accidentally giving a guest access to resources they shouldn't have. Essentially, this Device Group is for guests whose access has expired.

4. Hold or Revoke the Remove Access device group – For people that have been moved to the Remove Access group, you can choose to:
 - a) Hold – Allow the guests to stay until they require access again.
 - b) Revoke – You can revoke the Airwall Agent or Server licenses for the people in the group, which returns the agent and server licenses back into the license pool.

API Tip – You can revoke agents and servers in the API: Query for Airwall Agents with the “remove access” tag and revoke them if they no longer hold the grant access tag.

5. Add the “remove access” and grant access tags to the **Airwall Invitations** for the people you want to expire access

API Tip – You can also set the tags and send **Airwall Invitations** in the API.

Step 1: Create Guest Access tags

The first step to do is create tags for visitors to your Airwall secure network. You need to create two tags, one for guests with 4 hr access, and one for guests whose access has expired.

To create a tag for guests with 4 hr access:

1. In your Conductor, open **Tags** in the upper right corner.
2. Select **Create tag** and name the tag **GuestAccess4hr**.
3. Under **Who can use this tag?**, set it to **Any Admin users**.
4. Under **Tag color scheme**, choose a color. This example uses orange.
5. Set **Tag priority** to **1**. This tag takes priority over the **Guest Expired** tag.
6. Set **Expire tag usage after this duration** to **4h**. If you want to customize the time period, supported units are: y, M, w, d, h, m, s (default) with no spaces. For example: 4h30m50s.
7. Click **Create**.

To create tag for guests whose access has expired:

1. On the **Tags** page, select **Create tag**, and name the tag **GuestExpired**.
2. Under **Who can use this tag?**, set it to **Any Admin users**.
3. Under **Tag background color** and **Tag text color**, choose colors, and check the example for the result. This example uses red.
4. Set **Tag priority** to **2**. This tag takes secondary priority to the **GuestAccess4hr** tag.
5. Leave **Expire tag usage after this duration** set to **0s** (this indicates the tag is permanent).
6. Click **Create**.

Your tags page now has these two tags. Notice that the **Expire tag usage after this duration** setting is shown under **Usage TTL**:

Tags				
<input type="checkbox"/> Name	Ownership	Tag priority	Usage TTL	Auto-remove
<input type="checkbox"/> GuestAccess4hr	Any system admin users	1	4h	No
<input type="checkbox"/> GuestExpired	Any system admin users	2	0s	No

Step 2: Create Guest Access Smart device groups

Set up two Smart device groups that add people's devices as they connect.

Smart Device Groups are groups that are dynamically created and updated based on the rules you set up for the group. Along with tags, they allow you to automatically add devices people are connecting to groups based on what their Airwall Agent or Server has been tagged with.

You need to set up two groups that match your tags: one for guests with 4 hr access, and one for guests whose access has expired.

To create a Smart Device Group for guest 4 hr access:

1. In your Conductor, go to the **Devices** page.
2. Open the **Device groups** tab and select **Create group**.
3. On the **Device groups** page, name the group **Guest Access**.
4. On the **Guest Access** group page, under **Advanced properties**, check **Use rules to add devices**. This adds the **Rules** tab to the page.
5. Uncheck **Ignore auto-discovered devices until accepted**.
6. Open the **Rules** tab, click **Edit rules**, and then click **Add rule**.
7. In the **Rule Type** column, open the dropdown menu and select **Tag Match**. (Click the arrows to open the dropdown menu.)
8. In the **Arguments** column, select **Airwall**, and then right below the **Arguments** menu, click the edit icon .
9. Choose the **GuestAccess4hr** tag, then click the check icon  to set the tag.
- 10. Click Create.**

To create a Smart Device Group for guests whose access has expired:

1. In your Conductor, go to the **Devices** page.
2. Open the **Device groups** tab and select **Create group**.
3. On the **Device groups** page, name the group **Guest Expired**.
4. Under **Advanced properties**, check **Use rules to add devices**. This adds the **Rules** tab to the page.
5. Uncheck **Ignore auto-discovered devices until accepted**.
6. Open the **Rules** tab, click **Edit rules**, and then click **Add rule**.
7. In the **Rule Type** column, and select **Tag Match**. (Click the arrows to open the dropdown menu.)
8. In the **Arguments** column, select **Airwall**, and then right below the **Arguments** menu, click the edit icon .
9. Choose the **GuestExpired** tag, then click the check icon  to set the tag.
- 10. Click Create.**

You now have two Smart Device Groups (indicated by the  icon) for Guest Access:



The screenshot shows the 'Devices' page with the 'Device groups' tab selected. There are two entries in the list:

Device name	Overlay IP	MAC address	Airwall	Tags	Indicators
Guest Access	0				
Guest Expired	0				

At the bottom, there is a 'Sort by Name' dropdown and a note 'Items 1-2 of 2'.

Step 3: Create an overlay for Guest Access

Creating a new overlay used for guest access gives you the most control over the resources guests have access to.

1. In your Conductor, go to the **Overlays** page.
2. Select **New overlay network**.
3. Under **Select Network Topology**, select **Manual** and click **Next**.
For more information on other Network Topologies, see TBD.
4. On the **Create New Network** page, name the overlay **Guest Access**, and click **Finish**.
5. On the new **Guest Access** overlay page, by **Add devices**, click the plus sign (+).

6. Check the Guest Access group, and then also add the devices or device groups that you want guests to have access to and click **Add devices**.
7. Set trust between the Guest Access group and the devices you want them to have access to:
 - a) In the **Trust** column, select the Guest Access radio button.
 - b) Select the radio buttons for the devices guests can access.

For more information on setting device trust, see [Add and remove device trust](#) on page 360.

In this example, the Guest Access group has access to the Demo Network but cannot access the Internet access group.

Trust	Device name	Overlay IP	MAC address	Airwall
	Demo Network	0		
	Guest Access	0		
	Internet access	0		

You now have all of the pieces in place and are ready to send an invitation.

Step 4: Set up and send Airwall Invitations to guests

You can now create and send an invitation that automatically grants guest access to Airwall Agents and Servers connecting through that invitation.

1. In your Conductor, go to the **Airwalls** page.
2. Open the **Airwall Invitations** tab and click **Create Airwall Invitations**.
3. On the **Send Airwall Invitations** page, enter at least one email address for a guest, and click the Add icon .
4. Click **Next**.
5. Add a name for the profile to create on the Guest's Airwall Agent or Server.
6. Under **Install package location**, enter a link for the Airwall Agent to install. You can link to the installation package for the type and version of Airwall Agents you want them to use, or link to the latest Airwall Software Downloads page here //webhelp.tempered.io/webhelp/content/topics/downloads_latest.html.
7. Check the **Conductor URL**. It should already be added by default.
8. Under **Activation code expiration date**, leave the default settings and click **Next**.



Note: This is the expiration date for the invite only.

9. Under **Tags**, click the Edit icon , and select the Guest Access4hr tag.
10. Click the **Add an entry** box to open the tag list again and choose Guest Expired. With both Guest Access4hr and Guest Expired tags in the list, click on the add icon .
11. Click **Next**.
12. Review, add, or edit the email addresses or the invitation.
13. To send the invitations, click **Finish**.

As people accept your invitations, they are automatically given access for 4 hrs, and then removed from all access. For more details on how it works, see [How Expiring Access Works](#) on page 61.

What to do next

With access being granted and revoked automatically, all that you need to do to give new guests access is send them an invitation using the invitation you just created as a template. What you can do now:

- **Manage your Guest Expired devices** – You will probably need to eventually manage your guest expired devices to free up licenses or give them additional access.
- **Reuse Guest Airwall Invitations** - You can also reuse the invitation you sent to quickly invite new guests. For more information, see Reuse Airwall Invitations.
- **Renew Guest Access** – You can renew guest access for an additional 4 hours by just retagging the person's device. For more information, see Renew Access for Guest Expired devices.

Manage Guest Expired devices

For your guests in the Guest Expired Device Group, you can:

- **Leave them alone** – Keep them in the GuestExpired group indefinitely (this holds the license for them).
- **Revoke access** – Airwall Agent or Server and return the license to your pool of available licenses. For more information, see Revoke Access for Guest Expired devices.
- **Renew access** – Tag them with the GuestAccess4hr tag again to give them 4 hours of access again. For more information, see Renew Access for Guest Expired devices.

Renew Access for Guest Expired devices

1. In your Conductor, go to the **Airwalls** page.
2. On the **Airwalls** tab, click the **Tags** column header to sort by Tags, and find the devices that are tagged with `GuestExpired`, but not `GuestAccess4hr`.
3. Check the box to select the Airwall you want to renew access for.
4. At the top of the page, select **Airwall actions**, and then **Edit Tags**.
5. Under **Add Tags to selected items**, click the box with **Add an entry**, select the `GuestAccess4hr` tag, and then click the check to add the tag.
6. Click **Update**. The access countdown begins again, giving the guest 4 more hours of access.

Revoke Access for Guest Expired devices

1. In your Conductor, go to the **Airwalls** page.
2. On the **Airwalls** tab, click the **Tags** column header to sort by Tags, and find the devices that are tagged with `GuestExpired`, but not `GuestAccess4hr`.
3. Check the box to select the Airwalls you want to revoke access for.
4. At the top of the page, select **Airwall actions**, and then **Revoke**.

To re-instate a revoked Airwall, check the **Display Revoked Airwalls** box, check to select the revoked Airwall, select **Airwall actions**, and then **Re-activate**.

How Expiring Access Works

When people install Airwall Agents and Servers and accept **Airwall invitations** (clicking **Activate** in the email):

- Each person's Airwall Agent or Server is automatically added to both the `Guest Access` and the `Guest Expired` groups.
- Because the `Guest Access` tag takes priority, they are automatically added to the `Guest Access` Smart Device Group, and white listed to the devices or groups in your Guest Overlay for communication.
- The countdown for their 4 hr access starts.

When the 4 hrs is up, the `Guest Access` tag is automatically removed from the client, and the `Guest Expired` tag then takes priority and moves the Airwall Agent or Server to the `Guest Expired` smart device group, removing them from access to any overlay.

Connect People as Remote Access Users

You can create a remote access user to give a person access to your Airwall secure network using an Airwall Agent or Server. You can integrate with an LDAP user database, or add OpenID Connect authentication providers as shown in [Integrate Third-party Authentication with OpenID Connect](#) on page 208.

Set up remote access users to:

- Onboard users using membership in people groups (this gives them an activation code that they can click from the [Connect an Airwall agent](#) page)
- Authenticate a remote session on an Airwall Agent or Server
- Give users permission to view their connected Airwall Agent or Server status and see what remote devices they have access to (also via Connect an Airwall agent page)
- Enable and disable individual Airwall Agents and Servers authentication. For more information, see [Walkthrough: Onboarding Users with User Authentication](#).

1. In Conductor, go to **People**, and select **New Person**.
2. Fill in their details, and under **Role**, select **Remote Access User**.
3. At the bottom, choose whether to send the user a link to set their password, or create a password for them.

4. Select **Create person**.
5. **If you're onboarding users** – Add them to a user onboarding people group that provides them with an activation code. Then, once the user is logged in, they can download an Airwall Agent or Server, and activate their remote access. See [Set up a People Group](#) on page 74.
6. You can also add a person to an overlay from their **People** page.

People - RemoteUser

Info	
No tags in use	
API UUID	d09ad494-df04-4970-b242-f0107ca2ceef

People groups	
People group	Activation code
remote_access	None

Overlay networks	
Overlay network	Role
Untitled network	Member

- **If you've sent the user a link to set their password**, they'll get an email with a link to set a password.

- **If you created a password for them**, you'll need to send them their password.
- To allow a remote access user to access your Airwall secure network with an Airwall Agent or Server, you'll have to send them an activation code, or an Airwall Invitation. See [Connect People's Devices with Airwall Invitations](#) on page 54 or [Connect People's Devices with Activation Codes](#) on page 63.

Connect People's Devices with Activation Codes

Connecting people's devices with Activation Codes is similar to using **Airwall Invitations**. The only difference is you distribute the Activation Code or Codes yourself rather than automatically sending emails.

You send Activation codes to invite people to connect to your Airwall secure network. It can be as simple as generating and distributing the Activation codes. With a bit of preparation, though, you can also automatically set up device access and trust as people connect their devices.

The possibilities include setting up which Overlay networks people belong to, what groups they're a part of, which Airwall Edge Services and devices they can access, and when a person's access to your Airwall secure network expires.

Before you begin

- Group people by the types of access permissions they need.
- (Optional) Create **Airwall groups** for the people you want to add. For example, you may want Employees and Contractors Airwall groups.
- (Optional) Create tags for the types of people and access.
- (Optional) Create Smart Device Groups to automatically add people to Device groups as they activate their Airwall Agents and Servers. See [Manage devices dynamically with Smart Device Groups](#) on page 87.

By doing a bit more planning and preparation in the optional steps above, you'll save time in making sure people are able to access the resources they need.

1. Go to **Airwalls**, and open the **Airwall Invitations** tab.
2. *If you have already created Activation Codes or Airwall Invitations with the details you need*, you can open the drop down next to an invitation and select **Use as Template** to send a similar invitation to more people. *To create new Activation Codes*, select **New Airwall Invitations**, and select either **Download activation codes and distribute them manually** or **Download a single activation code that can be used many times**.
3. Enter the number of activation codes to generate, or how many times the single activation code can be used.
4. Select **Next**.
5. Enter the following options as needed. Setting these options automates more of the process for the people trying to connect:
 - **Generated Airwall name** – Sets the name the Airwall Agent or Server has in the Conductor when the user activates it. The default value sets it to the Airwall Agent or Server type. See the help when you select this box to see other options for autogenerated names.
 - **Activation codes should expire** – Check to have the activation codes expire
 - **Activation code expiration date** – If you've checked the box above, sets the date the Airwall Invitation expires.
6. Select **Next**.

7. Enter additional settings to automate people's access as their devices connect:

- **Overlay device IP network (CIDR)** – (Optional) The network from which to assign IP addresses to devices as they connect.



Note: If you use the same IP network in subsequent Invitations, IP addresses will keep incrementing. For instance, if you send out one Invitation starting at 192.168.1.15 with 10 emails and then another with the same IP with 10 emails they all just get a free IP from the network as they come online.

- **Overlay networks** – (Optional) The Overlay networks to add devices to.
- **Device groups** – Select the **Device groups** to add devices to.
- **Airwall groups** – Select **Airwall groups** to add devices to. For example, you might assign this group to the Employee, Admin, or Vendor group. Make sure this group has access to an Airwall Relay, if needed.
- **Tags** – Create or assign tags to people's devices. For example, if you're using tags to create Smart Device Groups that add people's devices to the right overlays, enter these tags now.

8. Select **Generate**.

9. Download or copy the Activation codes and distribute to the people you want to connect. To help your users receiving Activation codes to connect, point them to this help topic: [I have an Activation Code](#) on page 14.

To ensure people have access to the resources they need, add trust between their Airwall Agents and Servers and the resources they need to access on the overlays. And, if needed, add their devices to the Airwall Relay they'll use to access your Airwall secure network.

1. [Add and remove device trust](#) on page 360 on the Overlay between the device group for the people's Airwall Agents and the resources they need access to.
2. If needed, add the device group to any Relay rules they'll need to use to access resources. See [Set Up an Airwall Relay](#) on page 81.

Check Status of People Onboarding

You can check the status of people onboarding using Activation Codes or **Airwall Invitations** in the Conductor.

You can also run reports that show the overall status of your onboarding. See [Run Network Activity Reports](#) on page 101.

Check Activation Code Status

There are two ways to see the status of activation codes assigned to people from a People group:

On a person's detail page, look under **People** groups to see if they have unused activation codes from their People group membership.

On the **People** page, the far right column shows the following status icons. You can hover over the icons for additional details:

Icon	Meaning
	Authenticated user
	Unused activation code
	Expired activation code
	Person logged in in the last 24 hours
	Person logged in last week
	Person logged in more than a week ago
	Person has never logged in

Check Airwall Invitations Status

You can check the status of **Airwall Invitations** you've sent on the Airwalls page, **Airwall Invitations** tab.

- Select the arrow to the right of the **Created by** column to expand the status of **Airwall Invitations** and Activation codes created by that administrator and see the email addresses invited to join your Airwall secure network.
- The **Status** column shows how many **Airwall Invitations** are used and unused, and when expanded, shows provisioned and unused activations by email address.
- When the invitation is expanded, the **Airwall** column shows the Airwall Agents and Servers activated for each activated email address.

Created by	Created at	Email	Activation code	Status	Airwall	Expires at
▼ Admin	08/12/2020 3:03 pm	✉ j_banks@example.com ✉ j_banks@gmail.com	eb61c27d4a0d 8c01cf69e4	1 / 2 unused Managed Unused	j_banks's Airwall-Mac	08/26/2020 12:00 am

- The **Expires at** column shows how many **Airwall Invitations** are set to expire.

You can also select a **Filter by** tab at the top to filter by Unused, Managed, or Expired **Airwall Invitations**, or select **Refresh** to refresh the list..

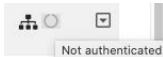
Check Remote Sessions

You can check the status of Airwall Agent remote sessions in these ways:

- On the Conductor page for a specific Airwall Agent, look under Remote Access:

The screenshot shows the 'Airwall agent - Windows-Airwall-Otto' page with the 'Remote Access' section open. It displays a session for 'Samwise Gamgee' with the IP '10.0.1.107'. The session was logged in at 06/26/2020 3:57 pm and expires at 06/27/2020 3:57 pm. The 'Edit settings' button is visible at the top right.

- The People page for a person shows details they are logged in.
- On the right side of the Airwall Edge Services list view, hover over the circle icon to see who's authenticated or Not authenticated. (Note that this icon only appears for Airwall Edge Services with authentication required.)



Here are some other icons that indicate status:

Icon	Meaning
🔌	Unused activation code
🔌	Expired activation code
🕒	Person logged in last week
🕒	Person logged in more than a week ago
🕒	Person has never logged in

Install Airwall Agents and Servers

Select your device for detailed installation instructions.

Once you've installed an Airwall Agent or Server, see [Connect to an Airwall secure network](#) on page 18.

Microsoft Windows or Windows Server: Install and configure an Airwall Agent or Server

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent or Server for Windows from the administrator of your Airwall secure network, or download the latest installation files from [Latest firmware and software](#) on page 431. Once installed, you configure a profile on the Airwall Agent or Server to link to the Airwall secure network.



Note: You can start and stop the Airwall Agent or Server service as needed. Keep in mind when an Airwall Agent or Server service is stopped, you won't be able to connect to anything on the protected network.

To install and configure the Windows Airwall Agent or Server:

1. Log into your Windows computer as an administrator.
2. Download and install the Windows Airwall Agent or Server from [Latest firmware and software](#) on page 431.



Note: If you are asked to install the TAP-Windows Provider as part of the installation procedure, click **Install** when prompted.

3. Once the installation is complete, the Airwall Agent or Server starts automatically.
4. Right-click the Tempered icon in the Windows System Tray
5. Select **Configure**
6. In the **Configure** window, do the following:

- a) Enter the IP address or host name of your Conductor. The default port setting is **8096**. If you have an activation code, enter it here.



Note: The **Device ID**, **Overlay Device IP**, and **Overlay Netmask** fields are read-only and configurable from the Conductor.

- b) Click **OK**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent or Server is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Windows Airwall Agent or Server, see [Connect with a Windows Airwall Agent or Server](#) on page 27.



Note: You may need to stop and restart the Airwall Agent or Server to allow it to connect to the Conductor. Right-click the Tempered icon in the Windows System Tray and select **Stop** to suspend the service or **Start** to resume.

Unattended Windows installation of an Airwall Agent or Server

In v2.0 and above, you can install the Windows Airwall Agent or Server in unattended mode as an Administrator.

To do an unattended install of the Windows Airwall Agent or Server you use an .msi file. This method runs the regular installer in silent mode, allowing you to do a silent install through domain (GPO, SCCM).

Here's the recommended command to use to do the unattended install:

```
msiexec /i <msi_file> /l*v msi_out.log InvitationCode=<invite_code>
Conductor=<conductor_URL>
```

For example:

```
msiexec /i AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi /
/l*v msi_out.log InvitationCode="575a52703294" Conductor="https://
my.conductor.com:8096"
```



Note: If you are not using DNS, you can replace the Conductor entry with its IP address. For example:

```
msiexec /i AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi /
1*v msi_out.log InvitationCode="575a52703294"
Conductor="https://192.168.56.2:8096"
```

Apple (OSX and macOS): Install and configure an Airwall Agent

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You must be an administrator of the computer to install and configure the Airwall Agent.



Note: Download the macOS/OSX installation files from the [Tempered Software Downloads and Release Notes](#) on page 431 Software Downloads section of Airwall help.



Important: In v2.2 and earlier, you may be required to install a TAP device driver. In earlier versions, the TAP driver's certificate may display a developer other than Tempered. If this occurs, you can safely click **Allow** and continue with your installation.

Once the installation is complete, the application starts automatically.

To install and configure manually:

1. To install the Airwall Agent locate the files you downloaded, double-click on them to run the installer, and follow the prompts.
2. Left-click the Tempered icon in the macOS menu bar
3. Select **Configure**.
4. On the **Airwall Configuration** page, do the following:
 - a) Select the plus (+) to add a new profile.
 - b) Under **Conductor**, enter the IP address or host name of your Conductor.
 - c) Under **Port**, use the default port setting of *8096*, unless your Airwall secure network administrator has told you to use a different port.
 - d) If you have an Activation code, under **Invitation**, enter the code. If you don't have a code, copy down or screenshot your **Device ID** and send to your administrator to activate your account.



Note: **Device ID**, **Overlay Device IP** and **Overlay Netmask** are read-only and configurable from the Conductor.

- e) Select **Save**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.



Note: You may need to stop and restart the Airwall Agent to allow it to connect to the Conductor. Left-click the Tempered icon in the menu bar and select **Stop Airwall** to disconnect or **Start Airwall** to connect.

For information on using your macOS Airwall Agent, see [Connect with an Apple \(OSX and macOS\) Airwall Agent](#) on page 18.

Perform an unattended macOS installation of an Airwall Agent

In v2.0 and above, you can perform a silent install on the Airwall Agent for macOS.



Note: This action requires administrator rights on the device.

To perform a silent install of the Mac client, from a terminal window, navigate to the location of the Airwall Agent installer package, and enter the command below:

```
sudo installer -pkg ./TemperedNetworksHIP.pkg -target /
```

Set your preferred network in the macOS Airwall Agent (HIPclient-OSX)

The macOS Airwall Agent (HIPclient-OSX) no longer uses the Network option, but instead automatically uses the network preferences on your macOS system settings.



Note: This action requires administrator rights on the device.

You can change the networks used by the agent by changing your macOS system settings.



Note: This setting is a system-wide setting, and affects network preferences for your entire mac system.

1. On your mac, click the WiFi icon, and select **Open Network Preferences**.
2. Under the list of available networks, click the gear icon, and select **Set Service Order**.
3. Drag the network options to set the network order you prefer, and then click **OK**.

2.2.3 macOS Airwall Agent Upgrade Instructions

If you have a previous version of the macOS/OSX Airwall Agent (formerly HIPclient) installed, follow these instructions to upgrade to 2.2.3:



Note: This action requires administrator rights on the device.

1. Check if you have this file on your Mac: /Applications/TemperedNetworksHIP.app. If not, you can upgrade as normal. If it's there, continue to step 2.
2. In your current Airwall Agent (HIPclient) menu, select **Configure**.
3. Note the Device ID and Conductor URL for each profile.
4. Go to the **About** menu, and select **Uninstall**.
5. Install the 2.2.3 macOS Airwall Agent.
6. Add a new profile for each of the Conductor URLs noted in Step 3. These new profiles will create new provisioning requests for each profile in the Conductor.
7. For the new profiles, a Conductor administrator needs to replace the old profiles with the new profiles. For more details, see [Replace an Airwall Edge Service](#).

Apple iOS: Install and configure an Airwall Agent

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for iOS from Apple's App Store.



Note: If you received an invite, follow the instructions in the email to install and configure your Airwall Agent. The instructions below are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Apple Store: <https://itunes.apple.com/US/app/id1233852249>.
2. Open the Apple iOS Airwall Agent.
3. From the menu, tap **Profiles**. Tap + to add a new profile.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it at the bottom.
6. Tap **ADD**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Apple iOS Airwall Agent, see [Connect with an iOS Airwall Agent](#) on page 20.

Android: Install and configure an Airwall Agent

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for Android from the Google Play Store. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.



Note: If you received an invite, follow the instructions in the email to install and configure your Airwall Agent. The instructions below are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Google Play store: <https://play.google.com/store/apps/details?id=com.temperednetworks.hipclient>
2. Open the Android Airwall Agent.
3. Add a new profile:
 - **v3.0 and later** – Scroll down to **Select Profile**, tap **MANAGE**, and then tap **+**.
 - **v2.2.12 and earlier** – From the menu, tap **Profiles**, and then tap **+**.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it.
6. Tap **ADD**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Android Airwall Agent, see [Connect with a Android Airwall Agent](#) on page 21.

Linux: Install and configure an Airwall Server

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Server for your Ubuntu, Centos, or Fedora Linux server from the administrator for your Airwall secure network, or from [Latest firmware and software](#) on page 431. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.



Note:

- For pre-3.0 versions, replace airsh with airctl.
- For pre-2.2.3 versions, see [pre-2.2.3 help](#).

1. Install the Linux Airwall Server package for your version of Linux. If your secure network administrator has not provided you with a download, you can download the package you need from [Latest firmware and software](#) on page 431.
 - **For CentOS 7 or 8 or Fedora 3.3:** `sudo rpm -i <CentOS or Fedora install package>`
 - **For Ubuntu 16.04, 18.04, or 20.04:** `sudo dpkg -i <Ubuntu 16 or 18 package>`
2. Create a profile: `sudo airsh profile create name=<profile name> conductor=<conductor_url> [act=activation_code]`.
You can optionally enter an Airwall Invitation activation code.
3. Make a profile the active one: `sudo airsh profile activate <profile name or number>`
4. Start the service: `sudo airsh service start`.



Note: If the service is already running, enter `sudo airsh service restart` to stop and start the service.

If you've used an Airwall Invitation or Activation code, once the Airwall Server is recognized by the Conductor, you should be able to start connecting to protected resources on the Airwall secure network. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on getting your Device ID, or using your Linux Airwall Server, see [Connect with a Linux Airwall Server](#) on page 26. For more Airshell commands, see [Linux Airwall Server Airshell commands](#) on page 309.

Linux Airwall Server or macOS Airwall Agent interface selection

The Linux Airwall Server and macOS Airwall Agent implement an interface auto-selection method. When you first install the Airwall Agent or Server, Linux or macOS determines the default gateway of the host and uses the associated network interface.



Note: Auto-selection is per profile.

Troubleshooting

If your Linux Airwall Server or macOS Airwall Agent is reporting as *online*, but doesn't seem to be working, check that the correct network interface is selected in the profile. This can be done by modifying `hip.conf` in the associated profile directory.

Example - List details of the active profile:

```
sudo airctl profile details --active

root@ubuntu-system-files:~# airctl profile details <profile_name>
profile_dir: profile1
profile_name: myprofile
network: ens4
deviceID:
overlay_device_ip:
overlay_mask:
conductor: myconductor.example.com:8096
log_level: info
```

You can find the settings for the active profile in the **profile1** folder under `/opt/tnw/profiles/profile1`. In that folder, open `hip.conf`, and change the `master_interface` key to the network interface you need.

Allow an Airwall Agent or Server to access your Airwall secure network

When a person configures an Airwall Agent or Server with your Conductor IP address or hostname, and are online with access to the **Conductor**, their Airwall Agent or Server will appear in the Conductor. How they appear depends on how they've connected:

- If they've activated their Airwall Agent or Server with an Airwall Invitation or Activation code, their Airwall Agent or Server is provisioned and configured as you specified when you set up the invitations or activation codes. You just need to license their Airwall Agent or Server and they will have access to the secure network.
- If the person is connecting manually, you get a provisioning request to allow the Airwall Agent or Server into your secure network. You need to provision and licensed the Airwall Agent or Server, and then add the person's device to the overlay networks and [Add and remove device trust](#) on page 360 for the resources they need access to.



CAUTION: When you're accepting provisioning requests, make sure that you know who is connecting and they are authorized to access your network.

If you need to revoke an Airwall Agent or Server, you can also disable trust in one click. For more information, see [Revoke and Reactivate an Airwall Edge Service](#) on page 419. Open the **Visualization** tab on an overlay network to get a visual view of trust relationships.



Note: You can also automate Airwall Agent trust using the API.

Manage Airwall Agents through an MDM (Mobile Device Management) solution

If you are using an MDM solution to manage devices for your organization, you can push installation and configuration of Airwall Agents to your managed devices.

The Airwall Solution currently supports managed configuration for Android Airwall Agents.

When you manage Airwall Agents with an MDM, the MDM can:

- Install the Airwall Agents on your managed devices.
- Create Airwall Agent profiles for your Conductor.
- Automatically start the Airwall Agent, which then reads the profile and connects to the Conductor.

The Airwall Agent prevents users from making any changes to a managed profile.

You can also distribute Activation codes through the MDM, or as Airwall Agents connect, you can grant the provisioning requests and manage the devices in the Conductor.

Before you begin:

- **Add the Tempered Airwall Agent to your MDM solution** – Follow the instructions for your MDM to load the Airwall Agent managed configuration. The values you can enter should be Profile Name, Conductor url, Port number, and Invite code. If you need to select the value type, set it to strings. All values are mandatory except for the invite code.
- **(Optional) Generate Activation Codes and put into your MDM solution** – To automatically provision users, generate Activation codes for the Airwall Agents you want to manage. To generate Activation codes, see [Connect People's Devices with Activation Codes](#) on page 63. To add these to your MDM solution, see your MDM instructions.
- **(Optional) Set up Dynamic variables in your MDM** – If you want to use dynamic variables in your profile names, set them up in your MDM following the instructions for your MDM.

Configure the managed profile for your Airwall Agents

These instructions are a rough guide and may vary depending on your MDM solution. See your MDM help for more detailed instructions.

1. In your MDM, open up the managed configuration for the Airwall Agent.
2. Configure and save the following values for the Airwall Agent profile:
 - **Profile name** – Enter the profile name you want your Airwall Agent profiles to have. If supported by your MDM , you can use dynamic variables to create profiles unique for each user.
 - **Conductor URL** – Enter your Conductor URL or hostname.
 - **Conductor Port** – Set the port default to 8096.
 - **Activation code** – (Optional) If you've set these up and it's supported by your MDM, enter a dynamic variable to insert each user's Activation code.
3. Save the profile, and save the configuration in your MDM.
4. Save and apply the managed configuration to managed devices following the instructions for your MDM solution.

You can change the profile information, except for the profile name, in the same way if you need to make changes to the managed profiles. If you change the profile name, the MDM creates a new profile on the Airwall Agents.

Automate the Airwall Agent or Server and Airwall Server using the API

Walkthrough - Onboard people to your Airwall secure network with User Authentication

How to set up global user/password authentication for Airwall Agents and Servers connecting to your Airwall secure network.

This walkthrough walks you through setting up authentication for all people connecting to your Airwall secure network.

 **Note:** This walkthrough covers globally onboarding people with authentication. You can also turn on authentication for individual Airwall Agents and Servers.

Supported Versions

Conductor v2.2.10 and later. This walkthrough is based on v3.0, so some things may be slightly different on earlier versions.

The basic steps are:

1. Require User authentication globally.
2. Onboard people using People Groups.
3. Add people as Remote Access Users.

These steps are covered in more detail below.

 **Note: For pre-2.2.8 Airwall Agents and Servers only:** There is an extra step to provide access at the end of this walkthrough.

Best Practice:

Finding the right balance between ease of use and security is an ongoing challenge.

This walkthrough shows how you can easily onboard and provide trust to a person, but you may choose to keep additional security checks in place, like granting the provisioning request based on the Device ID a person gives you.

A balanced option might include automatic onboarding, but only granting trust to a benign device that they can ping for communication verification and then provide final trust to secure environments once information has been verified verbally.

Step 1: Require user authentication globally

1. Go to **Settings** **Authentication**, and under **Settings**, select **Edit Settings** (in pre-v3.0, this is under **Global Airwall agent authentication settings**).
2. Check or set your authentication options:
 - Check **Require Airwall agent authentication** and select the option for all agents.
 - Under **Airwall agent authentication**, under **Airwall Agent Authentication Provider**, select **Username and password**, or an OpenID Connect (OIDC) third-party authentication provider, if you've set it up. See [auth openid connect.ditamap](#).
 - (Optional) You can also set a custom Session timeout or whether people need to log in when they restart their Airwall Agent

The screenshot shows the 'Global Airwall agent authentication settings' dialog box. It includes the following fields and options:

- Require Airwall agent authentication:** A dropdown menu set to "for all agents". Other options include "Require Airwall agent authentication for Windows servers" and "Require Airwall agent authentication for Linux servers".
- Session timeout:** Set to 24 hours.
- Airwall agent authentication provider:** Set to "Username and password".
- Retain session on service restart:** Checked.
- Require owner for Airwall agent authentication:** Checked.
- Auto-assign Airwall agent owner on login:** Checked.
- Warning message:** "⚠️ Updating the session timeout will not impact any existing sessions".
- Note:** "Settings with an asterisk (*) can be overridden on individual Airwall agents".
- Buttons:** "Save" (highlighted in yellow) and "Cancel".

The screenshot shows the same 'Global Airwall agent authentication settings' dialog box, but with a different configuration:

- Require Airwall agent authentication:** A dropdown menu set to "for all agents". Other options include "Require Airwall agent authentication for Linux servers" (which is checked) and "Require Airwall agent authentication for Windows servers".
- Session timeout:** Set to 24 hours.
- Airwall agent authentication provider:** Set to "Username and password".
- Retain session on service restart:** Unchecked.
- Warning message:** "⚠️ Updating the session timeout will not impact any existing sessions".
- Note:** "Settings with an asterisk (*) can be overridden on individual Airwall agents".
- Buttons:** "Save" (highlighted in yellow) and "Cancel".

For more information, see [Configure Authentication Options](#) on page 203. You can also require authentication per device on the Airwall Agent or Server page.

Step 2: Onboard People using People Groups

You may also want to [Import people using a CSV file](#) on page 51.

1. Set up a **People Group** on page 74, configuring the onboarding options you want to this People group to have. You can add people on the **People** tab, or add them to the group as you create users in the Conductor.

2. On the **User onboarding** tab:

- Check **Provide an activation code for each member**.
- Check **Send onboarding email to users** if you want to send emails automatically.
- Pre-configure the **General**, **Airwall**, and **Groups** settings for users when they onboard. Setting these options allows members of the group to activate their connections. For more information, see [Connect People's Devices with Activation Codes](#) on page 63.



Note: If you want to configure which version of the Airwall Agent they download, you can set that on the Conductor **Settings** page under **Global Airwall agent settings**.

On the People Groups page, you'll see your new group, and to the right, you'll see the Activation Code icon that indicates every person added to this group will receive an Activation Code. For more information, see [Connect People's Devices with Airwall Invitations](#) on page 54 or [Connect People's Devices with Activation Codes](#) on page 63.

Step 3: Add Remote Access Users

1. Add the people you want to connect to the Conductor. For Remote Access Users, see [Connect People as Remote Access Users](#) on page 61.
2. As you save each user, from each person's **People** page, add users to the people onboarding group created in Step 2.
 - a) Under **People groups**, select **Edit**.

People groups		Edit...
People group	Activation code	
mobile	None	

- b) Select the onboarding People group created in Step 2.
3. The people are sent an onboarding email. If desired, you can send them custom instructions, or point them to one of these help topics: [I have a "Finish Setting up my account" email](#) on page 14 or [I have an Activation Code](#) on page 14.
- As people click the link in the email to set their password and log in to the Conductor, they'll be directed to the [Connect an Airwall Agent](#) page where they can install an Airwall Agent or Server and activate their connections.

What's Next

You can get a report on remote sessions from **Visibility > Reports**. For more information, see [Run Network Activity Reports](#) on page 101.

You can see who's remotely logged into your Airwall secure network. See [Check Remote Sessions](#) on page 65.

You can also see which users have used their Activation codes. See [Check Status of People Onboarding](#) on page 64.

For pre-2.2.8 Airwall Agents and Servers only) Give the People group access

If you are onboarding people using pre-2.2.8 Airwall Agents and Servers you need to give the People group access by adding them to Overlays and Relay Rules.

On the Overlay these people need to access, add the People group you created as a **Viewer** (or pre v3.0, as a **Member**).

Select people or groups to view or edit your network

remo

Viewer Editor

cond_remote_users

Remote Access Users

Items 1-2 of 2

Close

Troubleshoot the Airwall Agent and Airwall Server

Follow the instructions below to resolve problems you may encounter using the software.

The Airwall Agent is not connected.

- Determine if the Conductor IP is configured. Follow the steps in the configuration section above.
- Verify that the Airwall Agent has not been given a certificate. Your administrator must grant a license in the Conductor. See the Conductor and Airwall Edge Service Administrator Guide for more information.

The Airwall Agent cannot contact a protected device

Configure the peer Airwall Gateway with an overlay network IP address and reestablish trust.

Set up a People Group

Set up a people group to make it easier to manage the people accessing your secure network.

Using a People Group, you can configure the User onboarding options, including Profile name, Conductor, and Airwall Gateways and resources these people have access to.



Note: If you are combining people groups with a third party authentication service such as LDAP or OIDC, you manage permissions in that service with group membership.

What you can do with People groups:

- **Manage trust** – You can assign trust dynamically to a people group using tags and a smart device group, or use the tag applied to Airwall Agents and Servers used by people in the group to easily find devices to add to a device group directly.
- **Onboard users** – You can use the **User onboarding** tab to send **Airwall Invitations** to people in the group and as they're added to the group. (You can also send invitations from the **Airwalls** page to the people currently in the people group).
- **Set Overlay network permissions** – Use the people to set overlay network editors and viewers.
- **Set groups to get alerts** – Send event monitor alerts to a people group.
- **Manage groups coming in from a third-party OIDC authentication provider** – Create people groups in the Conductor that exactly match the groups on your authentication provider to automatically add members of the group in the authentication provider to the group in the Conductor.

For more information on the types of users, see [Understand People Roles and Permissions](#) on page 49 or [Understand People Roles \(v2.2.13 and earlier\)](#) on page 50.

1. In Conductor, go to **People**, and open the **People groups** tab.
2. Select **New People Group**.

3. On the **Properties** tab: Set a name for this people group and add a description or tags, if desired.

Setting up a group for Third-party authentication: If you are managing people groups with a third-party authentication service, make sure the name matches your group on that service. Then, when you add people on that service, they are included in the people group when they log in.

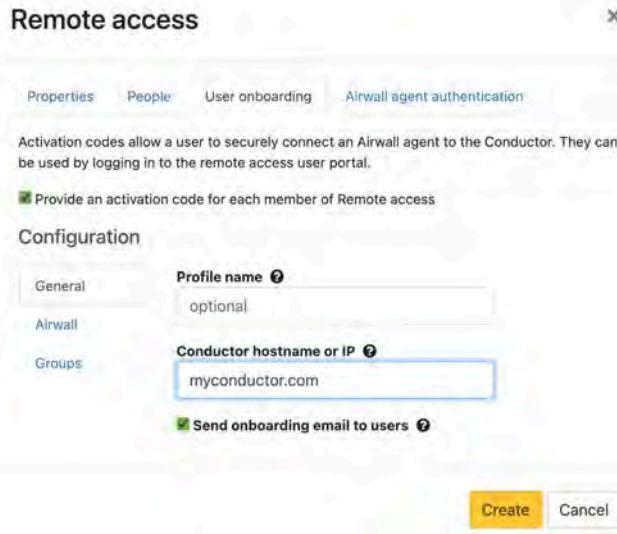
4. *If you are using a Third-party Authentication service, skip this step.* On the **People** tab: Select the people you want to be a member of this group.

The screenshot shows the 'People' tab of the 'Remote access' configuration. At the top, there are tabs for Properties, People, User onboarding, and Airwall agent authentication. Below the tabs, there are buttons for Show all, Members, and Non-members, with 'Members' being the active tab. A search bar contains the text 'test'. A dropdown menu labeled 'Role' is open, showing 'Name' as the sorting option. The user list is as follows:

User	Role
Test1	System Administrator
Test2	Remote Access User
Test3	Remote Access User
Test4	System Administrator
Test5	Viz Connector (beta)

Below the list, there are two small notes: 'Non-local users' people group membership must be managed on their authentication provider' and '** Roles in a people group that are set via an authentication provider reflect the most recent session'. At the bottom right are 'Create' and 'Cancel' buttons.

5. If you are using this group to onboard users, open the **User onboarding** tab, and check **Provide an activation code for each member of <groupname>**. Then, under **Configuration**, set up how to onboard the users added to this group:



- a) On the **General** tab:
 - **Profile name** – Set the name of the profile created on the Airwall Agent or Server for the user.
 - **Conductor hostname or IP** – Enter the Conductor hostname or IP.
 - **Send onboarding email to users** – Check to send new users of the group a notice that they have an activation code to connect.
- b) On the **Airwall** tab:
 - **Generated Airwall name** – Set the name to assign to the Airwall Agent or Server in the Conductor when the user activates it. The default value sets it to the Airwall Agent or Server type. See the help when you select this box to see other options for autogenerated names.
 - **Overlay device IP network (CIDR)** – (Optional) The network from which to assign IP addresses to devices as they connect.



Note: If you use the same IP network in subsequent Invitations, IP addresses will keep incrementing. For instance, if you send out one Invitation starting at 192.168.1.15 with 10 emails

and then another with the same IP with 10 emails they all just get a free IP from the network as they come online.

- **Tags** – Create or assign tags to people's devices as they connect. For example, if you're using tags to create Smart Device Groups that add people's devices to the right overlays, enter these tags now.

Remote access people group

Properties People User onboarding Airwall agent authentication

Activation codes allow a user to securely connect an Airwall agent to the Conductor. Activation codes can be used by logging in and visiting the "Connect an Airwall agent" page.

Provide an activation code for each member of Remote access people group

Configuration

General	Generated Airwall name <small>?</small>
Airwall	\${email_name}'s \${airwall_type}
Groups	Overlay device IP network (CIDR) <small>?</small> e.g. 192.168.16.0/20
Tags <small>?</small>	<input checked="" type="checkbox"/> Add an entry

Create **Cancel**

- On the Groups tab, you can add the devices people are using to connect to overlays and groups to automatically give them access to resources as they connect:
 - **Overlay networks** – (Optional) The Overlay networks to add people's devices to.
 - **Device groups** – Select the **Device groups** to add people's devices to.
 - **Airwall groups** – Select the **Airwall groups** to add people's devices to. For example, you might assign this group to the Employee, Admin, or Vendor group.

Remote access people group

Properties People User onboarding Airwall agent authentication

Activation codes allow a user to securely connect an Airwall agent to the Conductor. Activation codes can be used by logging in and visiting the "Connect an Airwall agent" page.

Provide an activation code for each member of Remote access people group

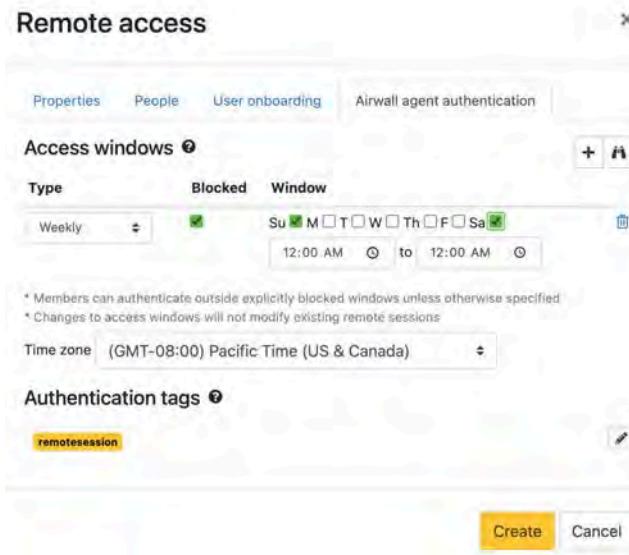
Configuration

General	Overlay networks <small>?</small> Add an entry
Airwall	Device groups <small>?</small> Add an entry
Groups	Airwall groups <small>?</small> Add an entry

Create **Cancel**

6. If this People group is using user authentication:

- a) If you want to grant or block access for this group at particular times, set up Access windows for the group. For more details, see [Set Times Authenticated Users can Access the Secure Network](#) on page 78.



- b) If you want to manage trust for the people group using tags, under **Authentication tags**, enter the tags you want to use to manage trust.



Note: These tags are applied to the Airwall Agent or Server when people in this group log in to authenticate their session. Tags are removed when the remote session ends. Combined with smart device groups, you can use these tags to dynamically create trust.

- 7. Select **Create**.

Set up User Authentication

How to set up user authentication for your Airwall secure network.

Here are the ways you can set up user authentication:

- [Integrate Third-party Authentication with OpenID Connect](#) on page 208
- [Configure LDAP authentication on Conductor and Airwall Edge Services](#) on page 219
- Use the local authentication in the Conductor

Related topics

- [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71
- [Set Times Authenticated Users can Access the Secure Network](#) on page 78

Set Times Authenticated Users can Access the Secure Network

Specify or restrict what days and times authenticated users can log in to access resources on your secure network by setting up Access Windows.

For example, you can use Access windows to:

- Allow one-time access for a vendor
- Restrict access to a resource except during defined maintenance windows.

Supported Versions

2.2.10 and later Conductor

Required Role

System and network administrators



Note: If a person is a member of multiple people groups with different Access windows, their session length will be either the longest available window, or the session length (which defaults to 24 hours), whichever is shorter. Multiple authentication tags will end according to the expiration you set (if any) for each Access window.

1. Log in to the Conductor as a system or network administrator.
2. Create or open the people group for which you want to control access. (To create a group, see [Set up a People Group](#) on page 74.)
3. Open the **Airwall agent authentication** tab.
4. Select **Edit** , then select the plus sign (+) to add an Access window.
5. For **Blocked**, leave clear to allow access, or check to block access for the specified window.



Note: If you set overlapping Allowed and Blocked Access windows for a People group, access will always be blocked during the overlapping times and removes authentication tags. However, if a person is in another People group that gives them access during that time, it does not block their access through the other People group's Access window.

6. For **Type**, select the type of window you want to create:
 - **Weekly** – Specify days of the week.
 - **Monthly** – Specify dates each month. For example, the 1st and 15th.
 - **Monthly day** – Specify a day each month. For example, the 2nd Tuesday of the month.
 - **Date range** – Specify a range of dates. You can use Date range to give someone one-time access to resources.
7. Under **Window**, choose the options for your chosen Access window type.

For example, for a Weekly Access window, you enter the days and time on those days to grant or block access. This Weekly Access window blocks access on the weekends:

Type	Blocked	Window
Weekly	<input checked="" type="checkbox"/>	Su <input checked="" type="checkbox"/> M <input type="checkbox"/> T <input type="checkbox"/> W <input type="checkbox"/> Th <input type="checkbox"/> F <input type="checkbox"/> Sa <input checked="" type="checkbox"/> 12:00 AM to 12:00 AM

* Changes to access windows will not modify existing remote sessions

Time zone (GMT-08:00) Pacific Time (US & Canada)

Authentication tags

remotesession

Save Cancel

8. Select the plus sign (+) to add more Access Windows for the group. Select the binoculars to leave editing mode.
9. Under **Time zone**, assign a Time zone for this People group's access windows. You can set different time zones for different People group's Access Windows.

10. If you want to manage trust for this People group using tags, under **Authentication tags**, enter the tags you want to use to manage trust.



Note: The Conductor adds the Authentication tags you've created for a people group to the person's Airwall Agent or Server when they authenticate, and removes the tags when they log out. You can see the authentication tags on a person's Airwall Agent or Server page under **Tags**. Combined with smart device groups, you can use these tags to dynamically create trust. See [Manage devices dynamically with Smart Device Groups](#) on page 87.

11. If you are creating a new People group, select **Create**. If you are editing an existing group, select **Save**.

Related concepts

[Manage devices dynamically with Smart Device Groups](#) on page 87

Use Smart Device Groups to greatly simplify the creation and management of large groups of devices. Dynamically add devices to a group by defining rules to create a Smart Device Group. Rules can match criteria such as organizational hierarchy, geographic location, or network domain. When you create a Smart Device Group, any new devices that match the rules you defined are added to the group automatically.

Related tasks

[Set up a People Group](#) on page 74

Set up a people group to make it easier to manage the people accessing your secure network.

Set up an Airwall Relay to Route Encrypted Connections

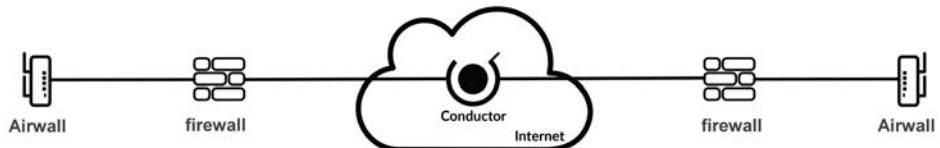
An Airwall Relay routes encrypted Airwall Edge Service connections across all networks and transport options, without modifying the underlying network, for secure end-to-end connectivity.

Supported on these Airwall Gateways:

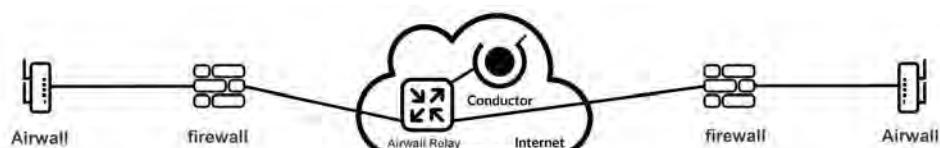
- **Physical** – 300 Series, 400 Series, and 500 Series
- **Virtual** – 300v on VMware ESXi, Hyper-V, RackSpace, Xen, and XenServer
- **Cloud** – 300v on Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud.

With an Airwall Relay in place, you can dynamically and easily network any device or group of devices across any public, private or hybrid network, including subnets that are located on separate underlays. The Airwall Relay brokers connections between Airwall Edge Services, based on policies set by the Conductor.

In the illustration below, two Airwall Gateways exist in different underlays. Each Airwall Gateway can connect to the Conductor, publish their IP addresses, and come online. However, communication between the two cannot occur as both Airwall Gateways do not have publicly available IP addresses.



To solve this limitation, add an Airwall Gateway acting as an Airwall Relay. In the Conductor, the Airwall Relay acts as a broker between the two Airwall Gateways.





Note: To set an Airwall Gateway up as an Airwall Relay, you must have an Airwall Relay license.



Note: If you have Airwall Agents or Airwall Gateways that are only getting a IPv6 address on cellular, and you want to connect to other Airwall Edge Services on IPv4, you need to have a relay policy set up on a dual stack (IPv4 + IPv6) Airwall Relay. To do this, set both IPv4 and IPv6 IP addresses on the same underlay on the Airwall Relay, and enable bypass:



Set Up an Airwall Relay

You can set up a compatible Airwall Gateway as an Airwall Relay to route encrypted traffic on your network.

You must have an available Airwall Relay license to complete these instructions. For help with licensing, see [How Airwall Licensing Works](#) on page 159.

1. In the Airwall Conductor, open the Airwall Gateway you want to act as an Airwall Relay.
2. On the **Airwall gateway** tab, select **Edit Settings**.
3. Under **Advanced Settings**, check **Allow Airwall to act as an Airwall relay**.
4. Select **Update Settings**.
5. [Configure Airwall Relay rules](#) on page 81 for that relay (or add to a group of relays that has policy set up).



Note: Setting an Airwall Gateway as an Airwall Relay automatically uses an available Airwall Relay license. If no licenses are available, you receive an error message.

Configure Airwall Relay rules

You configure Airwall Relay rules to establish secure connections between Airwall Edge Services that cannot directly connect.

You must have permission to edit policy for all of the Airwall Edge Services you are adding to the relay rules.



Note: You can also [Set an Overlay to Automatically Manage Relay Rules](#) on page 82.

1. In the Conductor, go to **Airwalls** and open **Airwall relay rules**.
2. Select **New relay rule (Create rule in pre v3.0)**, name the rule, provide a description, and select **Create**.
3. Scroll down in the list to find the rule you created.
4. In the Communicate via Airwall relay column, click the edit icon, and pick the Airwall Relay or Airwall Relay group you want to create a rule for, and select **Save**.
5. Under the **Airwalls** column to the left, select the Airwall Edge Services or groups in one area that you want to connect with the relay.
6. Under the **Airwalls** column to the right, select the Airwall Edge Services or groups in another area that you want to connect with the relay.
7. You can continue adding rules to connect any Airwall Edge Services that require a relay to communicate.



Note: Managed relay rules do not normally display on the **Airwalls>Airwall relay rules** tab. If you want to see them, you can go to **Airwalls > Airwall relay rules** and at the bottom right, check **Display system relay rules**.

Set an Overlay to Automatically Manage Relay Rules

You can easily manage the relay rules for an overlay by setting it to automatically create relay rules that allow the trust relationships in the overlay.

Supported Versions

Conductor 2.2.10 and later

Required Roles

System administrators

Network administrators with permissions to the overlay



Note: You must first set up an Airwall Relay before you can enable automatic relay rules.

You can also configure Airwall Relay rules manually. See [Configure Airwall Relay rules](#) on page 81.

1. Open the overlay you want to automatically manage your relay rules.
2. Under **Info** on the right sidebar, select **Edit Settings**.
3. On the **General** tab, enable the **Manage a relay rule based on this overlay network's configuration** option.
4. Choose the Airwall Relays or Airwall Relay groups that you want this overlay to use.
5. Select **Save**.

The overlay creates relay rules that allow communication between all Airwall Edge Services in the overlay. Note that you still need to set up device to device trust for them to communicate.



Note: Airwall Edge Services try to connect directly first, and only use the relay if they cannot connect directly.



Note: Managed relay rules do not normally display on the **Airwalls** page. If you want to see them, you can go to **Airwalls > Airwall relay rules** and at the bottom right, check **Display system relay rules**.

Manage Devices and Airwall Edge Services

Set up tags, groups, and Smart Device Groups to help you manage the devices connected to your Airwall secure network.

Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers

Reduce the traffic from Airwall Agents and Servers connecting to your Conductor by setting up disconnected mode. In disconnected mode, Airwall Agents and Servers connect to your Conductor at intervals – between 10 minutes and 12 hours (720 minutes) – to get updates when people are not actively using the connection.

By reducing the traffic on your Conductor, disconnected mode allows you to improve performance and scalability of your Airwall secure network.



Note: People using Airwall Agents and Servers can manually sync to the Conductor when in Disconnected mode.

1. Open the page for the Airwall Agent or Server that you want to enable disconnected mode for.
2. Select **Edit Settings**.
3. Under **Advanced settings**, scroll down to the bottom and check **Enable disconnected mode**.
4. Enter the time interval for the Airwall Agent or Server to reconnect to the Conductor.
5. Select **Update Settings**.

The Airwall Agent or Server you set disconnected mode on now disconnects from the Conductor, and reconnects at the specified interval to get configuration and trust policy updates. While in disconnected mode, the Airwall Agents and Servers show in the Conductor as not connected, and if you hover over the online status, they show they're in Disconnected mode and when their next connection is scheduled.



Note: In Disconnected mode, an Airwall Agent or Server:

- Can still connect to resources on your Airwall secure network.
- Gets policy and firmware updates the next time they connect.
- Do not publish underlay IP updates or status (health data, traffic stats, port status).



Note: Certain changes (such as underlay IP changes) can cause a disconnected Airwall Agent or Server to not be able to reach resources on your Airwall secure network. If this happens, the person using the Airwall Agent or Server can get the changes and reestablish their connection by either selecting **Sync Now** on their Airwall Agent or using the `conductor sync` Airshell command on their Airwall Server. For more information on Airshell for the Linux Airwall Server, see [Sync an Airwall Agent or Server in Disconnected Mode](#) on page 29.

Manage and organize with Tags

Use tags to manage and organize your Airwall secure network. You can tag most things in the Conductor.

You can tag:

- Airwall Gateways and Airwall Gateway Groups
- Overlay Networks
- Devices and Device Groups
- People

You can use tags to:

- **Simplify user onboarding** with **Airwall Invitations** or **Activation codes**. See [Connect People's Devices with Airwall Invitations](#) on page 54.
- **Search and filter** throughout Conductor.
- **Automatically add devices to Smart Device Groups** by creating a rule matching a tag. See [Use device groups and smart device groups](#) on page 354.
- **Set a trigger for an Event Monitor**. See [Monitor Activity with Events and Alerts](#) on page 101.
- **Set network policies**, including temporary network policies like expiring access. For an example, see [Walkthrough -- Send Expiring Guest Access Invitations](#) on page 57.
- **Revoke policy directly** from devices or Airwall Gateways without having to navigate to a network by deleting the tag that gives them access.
- Mark which assets are managed by which people.

You can tag items permanently, until you untag them, or set an expiration date, which untags an item after a period of time.

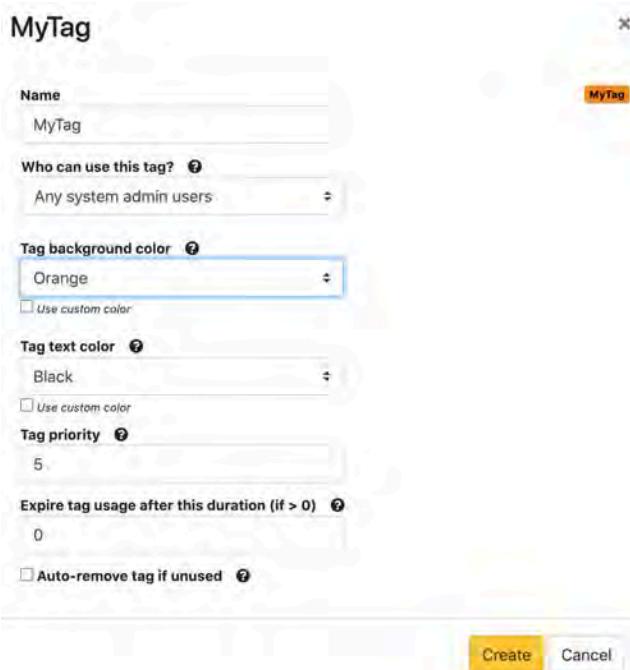
Create a Tag

To quickly create a tag, hover in an Tag column or box, and click the edit icon that appears. Enter a new tag, select the check mark or press **Enter** to add it, and then select **Save**.

To set advanced options on a tab, go to the Tags page:

1. In the upper right corner of the Conductor, select the Tag icon to open the **Tags** page.

2. Select **Create tag**.



3. Enter a Name for your tag.
4. Under **Who can use this tag?**, select the permissions you want to set for the tag.
5. Under **Tag background color** and **Tag text color**, choose colors, and check the example for the result.
6. Under **Tag priority**, set the priority for the tag. Use this to set relative priorities for tags. The tag with the lowest number takes precedence over tags with higher numbers.
7. Under **Expire tag usage after this duration**, set an expiration duration, if needed. Leave it set to 0 to make the tag permanent.
8. To remove the tag if it's not used, check **Auto-remove tag if unused**.
9. Select **Create**.

Related tasks

[Edit Tags](#) on page 84

[Delete Tags](#) on page 86

[Create or Manage Tags Inline](#) on page 86

Edit Tags



Note: You can only edit tags for items that you have permission to edit.

1. In the upper right corner of the Conductor, select the Tag icon to open the **Tags** page.
2. Open tag you want to edit.

3. The **Navigation** tab shows everything tagged with this tag. You can click the Name of an item to open it.

The screenshot shows the 'Auth0' interface with the 'Navigation' tab selected. A table lists three 'People groups' with their names, the user who tagged them, the time since they were tagged, and their expiration date. The 'Actions' and 'Properties' tabs are also visible at the top.

	Name	Tagged by	Since	Expires
People groups	cond_system_admins cond_READONLY_admins cond_NETWORK_admins		6.9mo ago 4.2mo ago 1.1mo ago	Never Never Never

At the bottom right are 'Save' and 'Cancel' buttons.

4. On the **Actions** tab, you can:

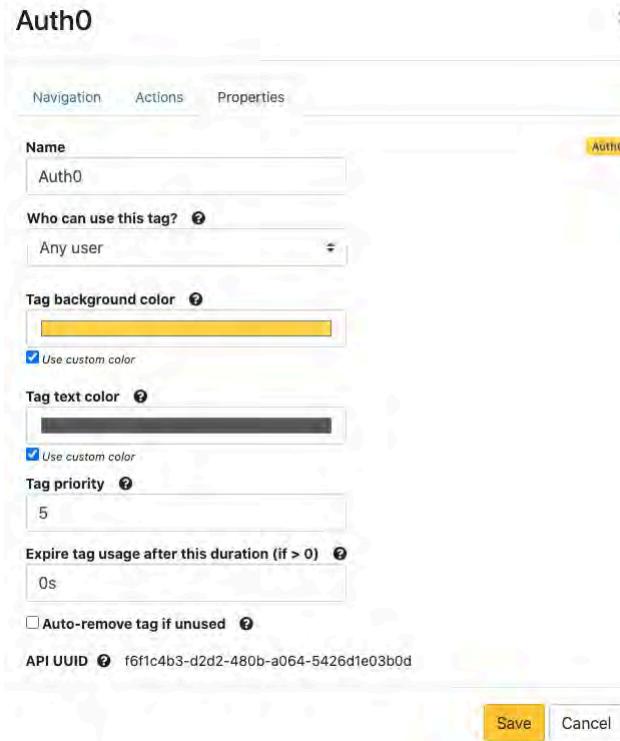
- Refresh** – Refresh expiration time for any expiring tagged items. You can check the expiration settings on the **Properties** tab.
- Enable** or **Disable** – Enable or disable communications for all tagged items. Select the confirmation message **Yes please...let's do this!** to continue, or select **Cancel** to cancel.
- Untag** – Remove the tag from all items, but not from rules, event actions, or user authentication.

The screenshot shows the 'Auth0' interface with the 'Actions' tab selected. It displays four options: 'Refresh', 'Enable', 'Disable', and 'Untag'. Each option has a brief description below it. At the bottom right are 'Save' and 'Cancel' buttons.

Refresh	Refresh expires-at time for all expiring tagged object relationships (based on current usage_ttl).
Enable	Enable communications for all tagged overlay networks, devices, device groups, Airwalls, and Airwall groups.
Disable	Disable communications for all tagged overlay networks, devices, device groups, Airwalls, and Airwall groups.
Untag	Remove this tag from all objects in the system (note: will not affect device group match rules, event actions, or user authentication tags)

At the bottom right are 'Save' and 'Cancel' buttons.

- On the **Properties** tab, you can change any of the settings for the tag. For descriptions, see [Create a Tag](#) on page 83.



- Select **Save** if you want to save any changes to the tag.

Create or Manage Tags Inline

You can access tags from several places in the Conductor, both from the tables on the **Overlays**, **Devices**, **Airwalls**, or **People** pages, and on the page for a specific resource, such as an Airwall Gateway.

You can tag items permanently, until you untag them, or set an expiration date, which untags an item after a period of time.

- Access the tag from one of these places:

- Next to Tags on some pages.
- By selecting **Edit Settings** on a page.
- On any page with a table that has a **Tags** column.

- Create or manage them inline:

- To add or create a tag** – Hover in the column and click the edit icon that appears. Type a new or existing tag, select the check mark or press Enter to add it, and then select **Save**.
- To remove a tag from a resource** – Click the X on the tag.
- To manage a tag** – Click the tag to open it, and edit on the **Actions** or **Properties** tabs for the tag. See [Edit Tags](#) on page 84.
- To navigate to a tagged resource** – Click the tag to open it, and select other items that have that tag to go there.

To delete a tag from the Conductor, see [Delete Tags](#) on page 86.

Delete Tags

You can delete tags individually, or delete several tags at once from the **Tags** page.

-

In the upper right corner of the Conductor, select the Tag icon  to open the **Tags** page.

2. Check the box next to one or more tags.
3. At the top of the page, open **Actions**, and select **Delete tags**.

Create standard device groups

Put devices into device groups so you can manage them as a group. If you want to create a smart device group where devices are automatically added if they match rules, see [Manage devices dynamically with Smart Device Groups](#) on page 87.

v3.0 and later

To create device groups:

1. Go to **Devices > Device groups** and select **New group**.
2. Enter a unique name for the group and, optionally, a description and tags for the group.
3. Select **Create**. The page for your new device group opens.
4. In the **Add Devices** box, enter a string to search for, check the devices you want to add to the group, and select **OK**.



 **Note:** You can also select the + (plus sign) to filter and select devices, including sorting by devices or bypass destinations.

Before v3.0

To create device groups:

1. Go to **Devices > Device groups** and select **Create group**.
2. On the **Properties** tab, enter a unique name for the group and optionally, a description.

 **Note:** If *Automatically recompute* is not selected, the Conductor determines when recomputing a rule is required and displays the  icon in the **Indicators** column of the device list. Manually recompute the group by selecting the drop-down arrow to the right of your device in the device list and select **Recompute group**.

3. Add any tags for this group.
4. On the **Devices** tab, check the box next to the devices you want to add to the group.

 **Note:** You can show all devices, show only members of the group, or show only non-members of the group, or filter the list of devices by entering text in the **Filter** field to quickly check the list or locate the devices you want to add.

 **Note:** In a standard device group, you add and remove members from this tab. In a Smart Device Group, this tab lists all devices added based on the Device match rules, and you cannot modify it directly.

5. Select **Create**.

Manage devices dynamically with Smart Device Groups

Use Smart Device Groups to greatly simplify the creation and management of large groups of devices. Dynamically add devices to a group by defining rules to create a Smart Device Group. Rules can match criteria such as organizational hierarchy, geographic location, or network domain. When you create a Smart Device Group, any new devices that match the rules you defined are added to the group automatically.

To find Smart Device Groups, go to **Devices > Device groups**. Look for the Smart Device Group icon (resembles an academic cap) .

To see an example, see [Smart Device Group example on page 92](#).

Create a Smart Device Group

You create a device group and then give it an ordered list of Device Match Rules to determine which discovered devices to add to your device group. When the Conductor discovers a new device, it checks the rules for all Smart Device Groups. If the device matches all of the Device Match Rules successfully, the Conductor adds it to that group. Be sure to review the [Best Practices for Smart Device Groups](#) on page 95 for help on setting great rules.

v3.0 and later

Follow this section to add a smart device group in v3.0 and later.

1. To create a Smart Device group, create a device group, go to the **Match rules** tab, and enable **Use rules to add devices**. Enabling this shows the **Device match rules** section.
2. Next to **Device match rules**, select the edit icon , and the next table row on the right, select **Add Rule**.
3. Set the rules you want to determine which devices are added to this group:

Order

Specify the order you want the rules run. You can receive very different results based on how you order your rules. For details, see [Rule ordering](#) on page 90.

Operator

Use an operator to determine the logic by which devices are added as members of the group. See [Rule operators](#) on page 90 for a list of operators.

Reverse (!)

The reverse option reverses the result of the operator. The [Smart Device Group example](#) on page 92 contains a device match rule that uses the reverse option as an example.

Rule type

Select the information you want to use to determine what devices are added to a Smart Device Group. See [Rule types](#) on page 91 for a list of rule types.

Arguments

Select the arguments, or options, for the rule type you selected.



4. To add additional rules, select **Add rule** again.

To delete rules, next to the rule, click the delete icon .

5. Under the rules table, check the rule options. It is best practice to keep both of these checked:
 - **Ignore auto-discovered devices until accepted** – Keep this box checked to only add discovered devices after they have been managed by a Conductor administrator.
 - **Automatically recompute after rules change** – Keep this box checked to recompute the device group whenever the rules are changed.
6. Set the Rule editor to a person with permissions to manage the devices in the Smart Device group.



CAUTION: If you disable **Use rules to add devices** on an existing Smart Device Group and click **Save**, the Smart Device Group reverts to a standard device group and the Device match rules are deleted. Devices added by the rule retain membership in the group but now you must add and delete devices manually using the **Properties** tab.

Set Device Match Rules

The screenshot below illustrates how you might construct a typical set of device match rules. These rules:

- Add all Airwalls in the Campus-West Airwall group, then,
- Add all devices in the Campus-East Airwall group, then,
- Remove all devices that are in the Instructors device group.

Order	Oper.	! Rule type	Arguments
10	+ include	<input type="checkbox"/> Airwall group	Campus-West
20	+ include	<input type="checkbox"/> Airwall group	Campus-East
30	- exclude	<input type="checkbox"/> Device group	Instructors



Note: If you change the order of these rules to exclude instructor devices first, it will exclude the Instructor device group first, then add Airwalls in the Campus-West and then Campus-East Airwall groups, which means instructor devices in those groups are added back in.

Before v3.0

Follow this section to create a Smart device group in earlier versions.

1. To create a Smart Device group, when creating a device group, on the **Rules** tab under **Use rules to add devices**, select **Enabled**. You can then create Device match rules.
2. Select the edit icon , and then select the plus sign (+).
3. Set the rules you want to determine which devices are added to this group (see descriptions in the v3.0 instructions).
4. To add additional rules, select the plus sign again.

To delete rules, next to the rule, click the delete icon .

5. Check the rule options as described in the v3.0 instructions.
6. Set the Rule editor to a person with permissions to manage the devices in the Smart Device group.



CAUTION: If you disable **Use rules to add devices** on an existing Smart Device Group and click **Save**, the Smart Device Group reverts to a standard device group and the Device match rules are deleted. Devices added by the rule retain membership in the group but now you must add and delete devices manually using the **Devices** tab.

Add rules to a Smart Device Group

To add rules to a Smart Device Group:

1. Navigate to **Devices>Device groups** in the Conductor.
2. Select a Smart Device Group from the list and click the **Rules** tab in the device group dialog
3. Click **Edit rules** to enter editing mode and then click **Add rule**
4. Enter the **Order**, **Oper.**, **!**, **Rule Type**, and **Arguments**

5. Click **Add rule** to continue adding rules or click **View rules** if you are finished and want to exit editing mode.
6. Click **Save**



Note: If any of the information is entered incorrectly, you will receive a validation error. Click **Edit rule** to return to editing mode.

Rule ordering

Device match rules are interpreted in order. You can get very different results based on how you order your rules.

This example illustrates how changing the order of rules can change which devices are added to the group.

Device match rules							
Order	Oper.	!	Rule type	Arguments			
10	+ include		<input type="checkbox"/> Airwall		Campus-West		
20	+ include		<input type="checkbox"/> Airwall		Campus-East		
30	- exclude		<input type="checkbox"/> Device group		Instructors		

The first rule adds all devices behind the **Campus - West** Airwall Gateway. The second rule adds any devices behind **Campus - East**. The third rule excludes all devices in the **Instructors** group, removing any Instructor Desktops from the group. This results in the following group membership:

- Classroom Desktop - 1st Floor Campus-West
- Classroom Desktop - 2nd Floor Campus-West
- Classroom Desktop - 3rd Floor Campus-West
- Classroom Desktop - 1st Floor Campus-East

If you reverse the second and third rule:

Device match rules							
Order	Oper.	!	Rule type	Arguments			
10	+ include		<input type="checkbox"/> Airwall		Campus-West		
20	- exclude		<input type="checkbox"/> Device group		Instructors		
30	+ include		<input type="checkbox"/> Airwall		Campus-East		

You get different results. The second rule still removes Instructor Desktops in Campus-West, but it doesn't remove them from Campus-East, since that rule hasn't run yet. When the third rule runs, any Instructor devices in Campus-East are included:

- Classroom Desktop - 1st Floor Campus-West
- Classroom Desktop - 2nd Floor Campus-West
- Classroom Desktop - 3rd Floor Campus-West
- Classroom Desktop - 1st Floor Campus-East
- Instructor Desktop - 1st Floor Campus-East

Since rules are processed in order, make sure you enter rules in an order that produces the intended result.

Rule operators

The following operators are available while editing rules:

Operator	Description
+ <i>include</i>	<p>Adds devices to the group that match this rule.</p> <p>Example: <i>include</i> CIDR 10.0.0.0/8</p> <p>Result: Include any devices with an IP address between 10.0.0.0 and 10.255.255.255.</p>
~ <i>filter</i>	<p>Filter the previous rule's results to only devices that match this rule as well. This operator is equivalent to <i>intersect</i> in set theory.</p> <p>Example: <i>include</i> Airwall Campus-West <i>filter</i> Range 10.0.0.100 10.0.0.106</p> <p>Result: Include devices in the group that are behind the Airwall Gateway <i>Campus-West</i> and have an IP address between 10.0.0.100 and 10.0.0.106.</p>
- <i>exclude</i>	<p>Removes devices that match this rule from devices added to the group by previous rules.</p> <p>Example: <i>exclude</i> Device Group <i>Instructors</i></p> <p>Result: Exclude any devices that belong to the <i>Instructors</i> group.</p>

Rule types

Here are the rules types you can select for device match rules:

Rule Type	Arguments	Description
CIDR	1	Match devices with IP addresses in the specified CIDR (Classless Inter-Domain Routing) group.
Overlay device IP network	2	Match devices matching the IP address and netmask specified (use dotted decimal notation, for example, 10.6.10.40).
Overlay device IP range	2	Match devices with IP addresses in the range specified by the two IP addresses (use dotted decimal notation).
MAC Prefix	1	Match devices with the specified MAC address prefix. Enter an empty field to match devices without a MAC address.
Airwall	1	Match devices under the specified Airwall Edge Service.

Rule Type	Arguments	Description
Airwall Attribute	2	<p>Match devices under any Airwall where the selected attribute matches the text you specify. The following attributes are available:</p> <ul style="list-style-type: none"> Name Description Location Model Product Platform Capability Code Cloud Attributes Version Hotfix List
Airwall Group	1	Match devices in the specified A drop-down list of existing Airwall group.
Tag match	1	Match devices with the specified tag.
Tag search	2	Match the selected type of objects (Airwall, Airwall group, or Device, or any object) that contain the specified tag.
Device Group	1	A drop-down list of existing device groups.

Edit existing rules in a Smart Device Group

Delete rules from a Smart Device Group

To delete a rule:

1. Select **Devices** in the Conductor.
2. Select the **Device groups** tab and select a device group from the list
3. In the device groups dialog, select the **Rules** tab and click **Edit rules**
4. To the right of the rule you want to delete, click the trash icon.



Important: There is no confirmation when deleting a rule. It is removed from the list immediately. If you delete a rule in error, click **Cancel** to revert to your last saved changes.

Smart Device Group example

The example below illustrates how a Device Group Rule (DGR) is interpreted (the screenshot is from pre-v3.0 Conductor, but later versions work similarly):

Campus Students

Properties Devices Rules

Use rules to add devices

Enabled **Disabled**

Device match rules

Order	Oper.	Rule type	Arguments
10	+ include	<input type="checkbox"/> Airwall group	Campus-West
20	+ include	<input type="checkbox"/> Airwall group	Campus-East
30	- exclude	<input type="checkbox"/> Device group	Instructors

Ignore auto-discovered devices until accepted (recommended)
 Automatically recompute after rules change (recommended)

Rule editor system

Save **Cancel**

There are two Airwall Gateways in this example, named **Campus - West** and **Campus - East**.

There are eight discovered devices, four behind the Airwall Gateway **Campus - West**, three behind the Airwall Gateway **Campus - East**, and one loaner laptop running an Airwall Agent.

<input type="checkbox"/> Device name	IP address	Airwall
<input type="checkbox"/> Classroom Desktop - 1st Floor	(⌚) 10.0.0.100	Campus-West
<input type="checkbox"/> Classroom Desktop - 2nd Floor	(⌚) 10.0.0.102	Campus-West
<input type="checkbox"/> Classroom Desktop - 3rd Floor	(⌚) 10.0.0.104	Campus-West
<input type="checkbox"/> Instructor Desktop - 2nd Floor	(⌚) 10.0.0.106	Campus-West
<input type="checkbox"/> Loaner Laptop 1	(⌚) 10.0.0.143	Loaner Laptop 1
<input type="checkbox"/> Public Desktop - North Wing	(⌚) 10.0.0.108	Campus - East
<input type="checkbox"/> Public Desktop 1 - South Wing	(⌚) 10.0.0.110	Campus - East
<input type="checkbox"/> Public Desktop 2 - South Wing	(⌚) 10.0.0.112	Campus - East

In this example, the rules dynamically add devices to the group that are behind the **Campus - West** Airwall Gateway or devices with intermittent connections to the network, while excluding devices from **Campus - East** and devices belonging to the Instructor Devices group.

10 **include** Airwall Edge Service **Campus-West**

The first rule adds all devices behind the **Campus - West** Airwall Gateway by using the *include* operator, the *Airwall Edge Service* rule type, and the selection *Campus - West* argument.

Device Match Rules				
Order	Oper.	!	Rule Type	Arguments
10	+ include		Airwall	Campus-West (1)

This rule matches the following devices:

Device name	IP address	Airwall
Classroom Desktop - 1st Floor	10.0.0.100	Campus-West
Classroom Desktop - 2nd Floor	10.0.0.102	Campus-West
Classroom Desktop - 3rd Floor	10.0.0.104	Campus-West
Instructor Desktop - 2nd Floor	10.0.0.106	Campus-West

Please note that there is one instructor device in the result, which is a member of the Instructor Devices group that we need to remove later.

20 **include [negate]** Airwall Edge Service **Campus-East**

The next rule adds any devices that are not behind the **Campus - East** Airwall Gateway by using the *include* operator, the negate option, *Airwall Edge Service* rule type, and the selection *Campus - East* argument. This captures any laptops running Airwall Agents that may intermittently require network access.



Note: In this example, you could remove the first rule and achieve the same result. It is included to illustrate the difference between the *include* operator plus the *negate* option and the *exclude* operator, later in this example.

Device Match Rules				
Order	Oper.	!	Rule Type	Arguments
10	+ include		Airwall	Campus-West (1)
20	+ include	!	Airwall	Campus - East (2)

These two rules will add one additional device, *Loaner Laptop 1*, to the result:

Device name	IP address	Airwall
Classroom Desktop - 1st Floor	10.0.0.100	Campus-West
Classroom Desktop - 2nd Floor	10.0.0.102	Campus-West
Classroom Desktop - 3rd Floor	10.0.0.104	Campus-West
Instructor Desktop - 2nd Floor	10.0.0.106	Campus-West
Loaner Laptop 1	10.0.0.143	Loaner Laptop 1

30 exclude Device Group *Instructor Devices*

The third rule excludes all devices in the **Instructor Devices** group by using the *exclude* operator, *Device Group* rule type, and the selection *Instructor Devices* argument.

Device match rules

Order	Oper.	Rule type	Arguments
10	+ include	Airwall	Campus-West
20	+ include	Airwall	Campus-East
30	- exclude	Device group	Instructors

This rule removes the device, *Instructor Desktop - 2nd Floor*, from the result:

Device name	IP address	Airwall
Classroom Desktop - 1st Floor	10.0.0.100	Campus-West
Classroom Desktop - 2nd Floor	10.0.0.102	Campus-West
Classroom Desktop - 3rd Floor	10.0.0.104	Campus-West
Loaner Laptop 1	10.0.0.143	Loaner Laptop 1

As more devices are discovered and managed by the Conductor, either behind an Airwall Gateway or running an Airwall Agent, the following actions will be taken by the rule:

- A device added to the **Campus - West** Airwall Gateway will be added as a member
- A device added to the **Campus - East** Airwall Gateway will not be added as a member
- Any device running an Airwall Agent will be added as a member
- Any device added to the *Instructor Devices* group will not be added as a member

Delete a Smart Device Group

To delete a Smart Device Group:

1. Go to **Devices**→ **Device groups**
2. Select the drop-down to the right of the device group you want to delete, and click **Remove group**

Best Practices for Smart Device Groups

Create easy-to-use, effective Smart Device Groups by following these recommendations to ensure your rules are constructed properly.

Use Smart Device Groups only when necessary

Smart Device Groups are very powerful and can be instrumental in helping you to manage a large number of devices, but not every group should be a Smart Device Group. Generally, you should manage device group membership manually when:

- There are no complex patterns to match
- Devices are easily differentiated, such as cameras or Web servers
- You are creating denylists and allowlists

Create Smart Device Groups for frequently used matches

For ease of management, avoid repeating the same logic in multiple Smart Device Groups. It is best to create a Smart Device Group and reuse that group in other Smart Device Groups using the Device Group rule type. For example, if you capture devices from a particular set of Airwall Edge Services, consider creating a Smart Device Group for that purpose and including it in other Smart Device Groups that require it.

There are a few considerations you want to keep in mind when nesting device groups:

- If a device group changes membership, any Smart Device Groups that refer to it in a Smart Device Group's Device Match Rules will need to be recomputed.
- A Smart Device Group included in another Smart Device Group does not trigger the parent group to recompute unless it also is set to automatically recompute. For example, standard device group *DG-Seattle* is included in smart device group *DG-Washington*, which is not set to automatically recompute. *DG-Washington* is included in *DG-UnitedStates*, which is set to automatically recompute. If a device is added to *DG-Seattle*, neither Smart Device Group will recompute because *DG-Washington* is not set to autocompute and *DG-UnitedStates*, which is set will not detect any changes from *DG-Washington*.

Exclude what you don't require as soon as possible

If your Device Match rules create a large result set, consider excluding what you don't need as early as possible, starting with the largest sets first. For example **US Servers exclude West Coast Servers exclude Washington State Servers** is more efficient than **US Servers exclude Washington State Servers exclude West Coast Servers**.

Maintain exceptions separately

Keep it Smart: If there are exceptions (that is, a "denylist") of devices to exclude from a smart group, maintain a separate denylist device group containing these devices rather than abandoning the rules and manually removing the devices from the group. For example, when troubleshooting, or as bad actors emerge in the network, add them to the denylist device group, and then add a rule to the end of your device match rules to exclude that device group from all of your Smart device groups.

Negation is more costly on system performance

If you negate a rule type, the Conductor requires extra processing for every device in a device set. If you choose to use negation in your Device Match Rules (DMRs), consider creating a separate Smart Device Group that stores the result of the negation rule. You can then use this separate group in multiple Device Group Rules with increased system performance.

Use more efficient rule types if possible

To construct Smart Device Groups that run as efficiently as possible, whenever possible, use device match rules for device groups, Airwall Edge Services, and Airwall Gateway groups.

Disable unused rules

Remove or disable unused Smart Device Groups, or have auto-compute disabled until you plan on using them in the future. If left active, they will continually process their rules and may impact performance if changes occur that involve a large number of devices.

Create Airwall Edge Service groups

If you are managing a large number of Airwall Edge Services, you can create **Airwall groups** in the Conductor to simplify administrative tasks.

Once you have **Airwall groups**, you act on them in groups:

- Reboot
- Update firmware

- Install a hotfix
- Disable network communications
- Do [Bulk Configuration of Airwall Edge Services](#) on page 314 (you can also select individual Airwall Edge Services for bulk editing)



Note: You can only add Airwall Edge Services to a group if you have permissions to edit them.

To create an **Airwall groups**:

1. Go to **Airwalls**.
2. Check each Airwall Edge Service you want to add to the group.
3. In v2.2.8 and earlier, select **Create Group**.
In v2.2.10 and later, select **Actions**, then **New group from selection**.
4. Enter a name, description, and tags, and if it's for an Airwall Relay, check **This group is an Airwall relay group**.
5. If you want to the group to have network communication disabled when it's created, under **Network communications**, select **Disabled**.
6. Go to the **Airwalls** tab to add additional Airwall Edge Services.
7. Select **Create**.

See MAC address OUI (Manufacturer) Information for Devices

The MAC address OUI (organizationally unique identifier) column shows the manufacturer names for your devices, determined from their MAC address.

1. In the Conductor, go to the **Devices** page and **Devices** tab.
2. Look at the OUI column in the **Devices** list, or open a device page and the OUI is shown under **MAC address**.

If the manufacturer list seems to be out of date, see [Update the MAC address \(OUI\) \(Manufacturer\) List](#) on page 413.

Search for or Sort Devices by MAC Address OUI (Manufacturer) Name

You can search for devices by the MAC address OUI identifying the manufacturer name for asset management.



Note: If you are not seeing some manufacturers, you may need to [Update the MAC address \(OUI\) \(Manufacturer\) List](#) on page 413.

To search by manufacturer name

There are two ways to search by manufacturer name:

- **In the ConductorSearch box** at the top right, enter a manufacturer name. Select from the list of matching devices that appears to open that device page.
- **On the Devices page**, in the Filter box, enter a manufacturer name. The **Devices** list is filtered to devices from that manufacturer.



Note: Search finds the manufacturer's name in any field, so if the manufacturer name appears in other areas, they will be included.

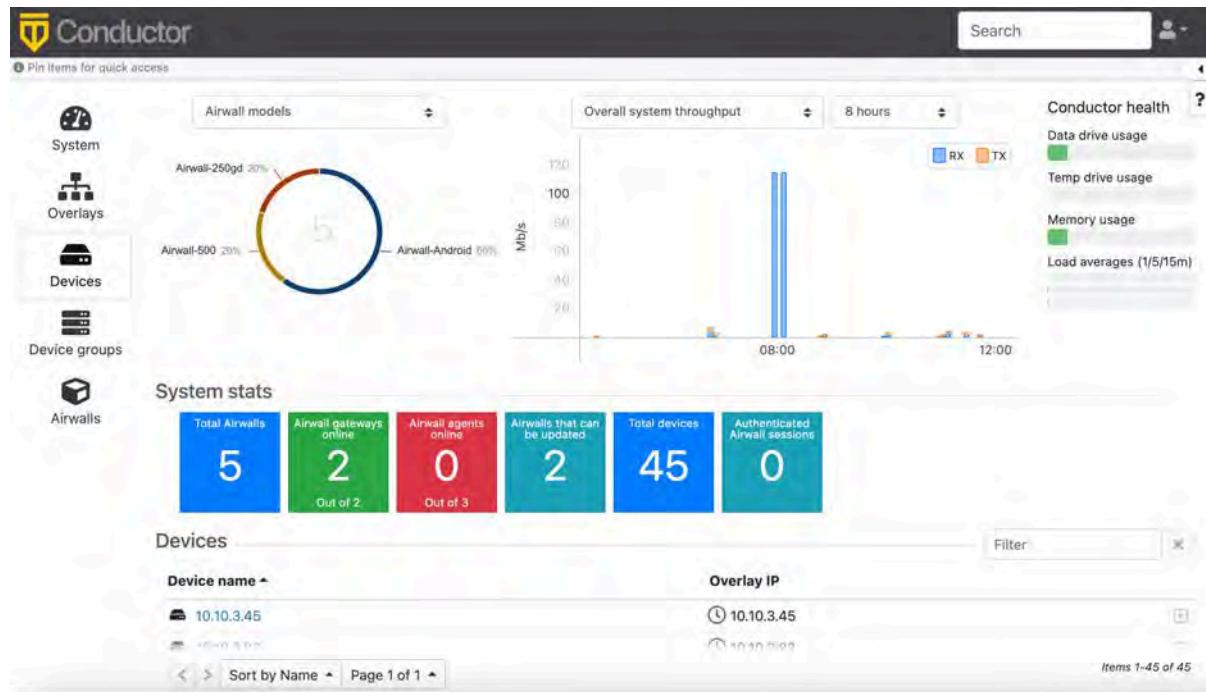
To sort by manufacturer name

On the **Devices** page, in the **Devices** list, click on the **OUI** column header to sort the list by manufacturer.

Manage Overlay Networks in Streamlined View

If you are a Network administrator using the streamlined view in the Conductor, the parts of the Conductor that you don't have access are hidden so you can more easily navigate and manage your overlay networks. You can more easily access your overlays and the devices, Device groups, and Airwall Edge Services in those overlays. Depending on your permissions, you may also be able to see unmanaged Airwall Edge Services.

Here's an example of the devices page in the streamlined view. Select a tile from the System stats to manage, or look below for a list you can click to go to a specific page:



Note: To check your permissions, select your profile icon (in the upper right), and selecting **Preferences**. You can see your permissions under **User permissions**. For permissions help, contact a Conductor System administrator.

See Airwall Edge Service Information and Status

Supported Versions

2.2.8 and later

There are several ways to see information and status on the Airwall Edge Services connecting to your Airwall secure network.

All of the information and status for an Airwall Edge Service is shown when you select one to display its page. Some of that information is also available on the **Dashboard** and **Airwalls** page listings.

The following sections cover where to find some of the most commonly-needed information.

Airwall Status, Model, and Firmware

The **Status** column and field display information such as whether the Airwall Edge Service is Enabled (provisioned and managed), Unmanaged, or Revoked, and the progress of firmware updates.

Status

	192.168.56.128	
Firmware Update: [missing "en.endbox.states.substates.Starting" translation]		
	61% - Firmware Update	



Note: Expanded status messages are available in Conductor v2.2.10 and later.

The **Model** column and **Model** and **Firmware** on an Airwall Edge Service page shows what kind of Airwall Edge Service it is and what version of the firmware it is currently running.

Most of the statuses are self explanatory. For details, see [Airwall Edge Service Statuses](#) on page 100.

Where to See Status and Information

The following sections show different ways you can see status for one or multiple Airwall Edge Services.

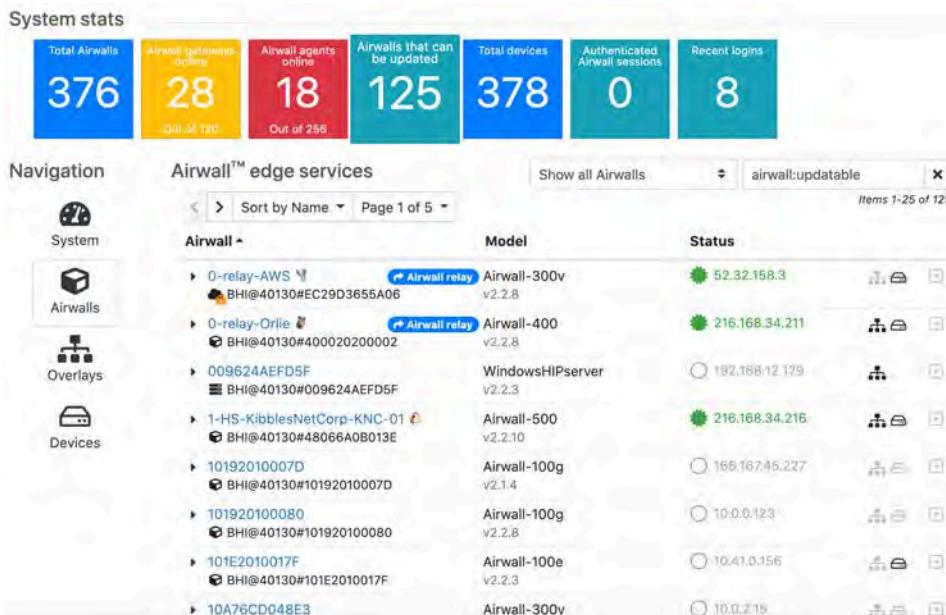
On the Dashboard

The Conductor Dashboard has several ways to see what Airwall Edge Services are connecting, and what their status is.

- **The Airwall Donut Graph** – On both the Airwall models and Airwall versions graphs, click on a donut section to see what Airwalls are that model or have that version installed in the **Navigation Airwalls edge services** section.



- **System stats** – Click on any stats tile to see more details **Navigation Airwalls edge services** section.



On an Airwall page

Open an Airwall to see more detailed status and information.

Airwall gateway - 0432447A6A97 (unmanaged)

Airwall gateway	
Status	 Unmanaged
Member of	The Airwall gateway must be managed before it can participate in any networks
Online status	 10.0.2.5
Published IPs	10.0.2.5
Tags	
Name	
Location	
Description	
Hostname	hs300v-0432447A6A97
UID	BHI@40130#0432447A6A97
API UUID ⓘ	b8ddf614-038f-46f5-8567-1fba748a817a
Serial number	0432447A6A97
Model	Airwall-300v
Firmware	Version 2.2.2

Airwall Edge Service Statuses

Information on the statuses you might see for an Airwall Edge Service. Some of these statuses are not available in v2.2.8 and earlier.

Airwall Agent authentication

The person using this Airwall Agent to connect is required to use authentication.

Airwall Relay

This Airwall is running as an Airwall Relay.

Disabled

Policy configuration is disabled.

Disabled by group

The Airwall group has communication turned off.

Enabled

Policy configuration is enabled.

ha primary

High-availability active (primary) Airwall Gateway

ha secondary

High-availability standby (secondary) Airwall Gateway

Locked out

User authentication has been locked out due to too many authentication attempts.

Revoked

This Airwall has been revoked.

Transparent

Airwall Gateway is in transparent mode.

Unmanaged

Airwall has connected to the Conductor but is not managed yet. You must provision and manage before you can add it to overlays.

Monitor Activity and Connections

Monitor activity and connections to your Airwall secure network with Conductor Event monitoring and alerting.

Roles

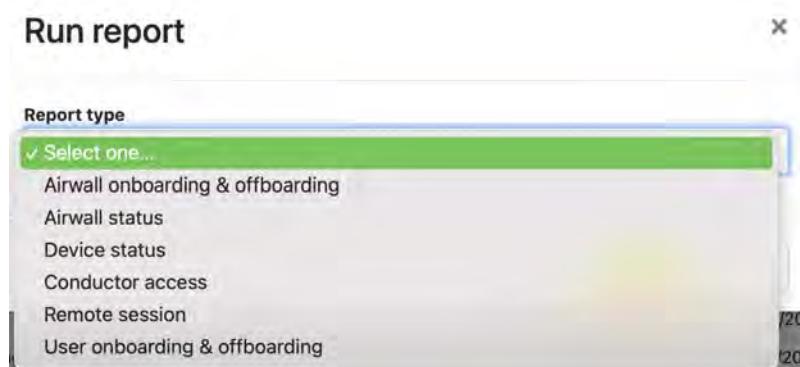
All Administrators for the overlays they have access to

Run Network Activity Reports

Run reports on different types of activity on your Airwall secure network.

You can create reports for the following network activity:

- Onboarding and offboarding of Airwall Edge Services or users
- Status of Airwall Edge Services or devices
- Conductor local or remote access



Note: You can also check the status of an individual. See [Check Status of People Onboarding](#) on page 64.

1. To run a report, go to **Visibility > Reports**.
2. Select **Run Report**.
3. Select the type of report to run, and enter any options.
4. Select **Run**.

The report you selected runs and then opens the report results.

View, Download, or Delete a Report

To view, download, or delete a report:

1. Go to **Visibility > Reports**.
2. In the list of Reports, find the report you want, and open the menu (click the down arrow on the right).
3. Select **View, Download, or Delete**.

You can also download or delete a report when viewing it.

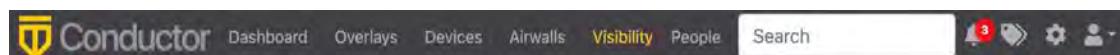
Monitor Activity with Events and Alerts

Use Events Monitors and Conductor-generated Alerts to create triggers to collect, analyze, and signal events that help you monitor activity and health of your Airwall secure network.

Roles

All Administrators. As a network administrator, you can view and manage event monitors and alerts for the overlays you manage.

To check or set Alerts and Event Monitors, open the **Visibility** page, or click the Bell icon (that indicates if you have alerts) in the upper right corner of the Conductor.



On the **Alert notifications** tab, you can view and take action on alerts.

On the **Event Monitors and actions** tab, you can create, edit, and view the event monitors you've created.

Alert level	Alerted at	Monitorable	Subject	Message
◆ Info	7/27/2021 3:36 PM	temperedtest's Airwall-Android	Airwall 'temperedtest's Airwall-Android'	has been automatically provisioned and managed using an activation code.

See and Manage Alerts

You can see and manage the alerts for overlays you have permission to see at **Visibility>Alert notifications**.

The **Alert notifications** tab shows both the default alerts from the Conductor, as well as the alerts set as actions for triggers on the Event monitors and actions.

You can choose to view alerts, or acknowledge, delete, or both acknowledge and delete alerts.

- **Acknowledge** - When you acknowledge an alert, you acknowledge it for everyone who received that alert. You can add a comment if desired. Other administrators will see the alert has been acknowledged.
- **Delete** - When you delete an alert, you are only deleting for yourself. Other administrators will still see the alert.
- **Acknowledge and Delete** - Do both.

To set which alerts send you emails, see [Set your Email Alert Level](#) on page 103.

Manage Alerts from the Visibility page

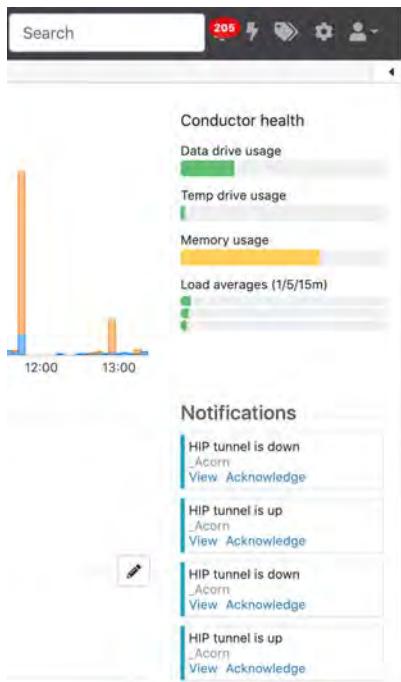
1. Click the Alerts icon to open the **Alerts notifications** tab with a list of alerts.
2. Check the box next to one or more alerts, then at the top of the table, select **Alert actions**, and select how to handle the alert.

Best Practice:

- *Acknowledge* alerts to indicate that you have checked out the alert and done what is needed to handle it, so other administrators know they don't need to.
 - *Delete* alerts that are not ones you need to handle, or that you no longer need to see.
3. Alternately, you can select the drop down on any alert to view or manage the alert.

Manage Alerts from the Dashboard

1. On the Conductor **Dashboard**, you can see alerts under **Notifications** on the right sidebar under the **Conductor health** section.



2. You can select **View** or **Acknowledge** to manage the alert from the Dashboard.

Set your Email Alert Level

Typically, you change your alert level temporarily for support, or to get more insight into what may be happening on your network for troubleshooting. This setting controls the level (and therefore number) of alerts that trigger an email to you when it occurs. If you're a Conductor system administrator, you can also set the level for other Conductor admins.

The default level is None.

In your Conductor profile, you can choose what level of alert triggers an email being sent to you. You can also set the email address and subject prefix for the email.

1. Open the Profile menu  in the upper right, and select **Preferences**, or go to the **People** page and select yourself, or, if you have permissions, select an existing person or [Add a Person](#)
2. Select **Edit Settings**.
3. Under **Alert email trigger level**, select the alert level to receive email notifications for: **Info** (everything), **Warning** (Warnings and errors), or **Error** (Errors only).
4. Select **Update Settings**

Create an Event Monitor

Create event monitors to help you manage and maintain the health of your Airwall secure network.

Best Practice: Set up Event Monitors to alert when an Airwall Edge Service goes offline.

Some types, models, and versions of Airwall Edge Services do not support all of the monitors. For example, Airwall Agents and Servers don't support remote monitors (ones that run on the Airwall Edge Service), but do support monitors that run on the Conductor.



Note: If you select a group to monitor that contains Airwall Edge Services that don't support the monitor, the monitor ignores the ones that don't support it, but will still trigger for the ones that do.

1. Go to **Visibility > Event monitors and actions**.

2. Select **New event monitor**.
3. Select a **Monitor type**, fill in the options for that type of event monitor, and then click **Create**.
4. On the **Actions** page, add actions that you'd like to happen for this monitor.

Best Practice: To make sure you're notified about an event, at a minimum, create an **Alert** Action for the monitor and under **Admins to receive this alert**, add a people group for the Admins who should see the alert.

5. After adding each action, select **Create** to add it to the **Action** list.

6. When you're done adding actions, select **Finish**.

For information on permissions and alerts, see [Set who sees Event Monitors](#) on page 104.

Set who sees Event Monitors

Set who sees alerts and event monitors



Note: Make sure the people you are adding to an event monitor have permissions that allow them to see the alert. See [Understand People Roles \(v2.2.13 and earlier\)](#) on page 50.

You set who can see an event monitor when you create or edit it. The person or people group must also have permissions to the overlay the monitor is set for.

Best Practice: When you create an Alert Action for the monitor, under **Admins to receive this alert**, add a people group for the Admins in the overlay who should see the alert.

See [Create an Event Monitor](#) on page 103 for details.

Monitor Connections to your Airwall secure network

The Conductor has several ways to monitor the people, Airwall Edge Services, and devices that are connecting to your Airwall secure network.

Monitor Connections from the Dashboard

The graphs and **System stats** tiles on the Conductor dashboard give you several quick views into the status of your Airwall secure network.



Note: Select a tile from **System Stats** to open up a more detailed view below under **Navigation**.

For more details, see [The Conductor Dashboard](#) on page 32.

Monitor and Manage Remote Sessions

1. In the Conductor, go to **People**.
2. Filter the people list, if desired.
3. In the **People** list, look at the clock icons at the end of the row. The clock icon shows by color the last time the person signed in, and you can hover over it to see the time and date they last signed in:

Icon	What it means
	In the last 24 hrs
	In the last week
	More than a week ago
	Never



Note: If you see a plug icon, it's an indicator of the state of user onboarding. See [Monitor User Onboarding](#) below for more details.

You can also open up the page for a person, and see their connected devices under People groups on the right. Click to open up any connected Airwall Agent or Server (that you have permissions to see), and review or end a remote access session.

- **To review the remote access session**, see the details in the **Remote Access** tile.
- **To end the remote access session**, select **End remote access session**.



Note: The Remote Access tile only appears when there is an active remote session.

Airwall agent - jbanks_mac

Status: Enabled

Member of: Overlay networks: WFH-Corp; Airwall groups: None; Airwall relay rules: breakathon

Online status: 192.168.0.6 (Source IP: 67.170.79.148)

Published IPs: 192.168.0.6

Tags: inside_sales

Remote Access

End remote access session

Joe Banks(jbanks_mac)
(Login: 07/08/2020 12:47 pm, Expires: 07/08/2020 1:47 pm, From: "mbp")

Monitor User Onboarding Airwall Invitations and Activation Codes

Once you've sent out **Airwall Invitations** or started onboarding with Activation Codes, you can review which activations have been accepted, are still active, or have expired.

1. In the Conductor, go to **People**.
2. Filter the people list, if desired.
3. In the **People** list, look at the plug icons at the end of the row. The plug icon indicates the person has been sent an activation codes or Airwall Invitation. Hover over the icon to see how many are active.:

Icon	What it means
	If the plug is black, the person has unused, non-expired activation codes or invites available.
	If the plug is grey, the person has used all of their activation codes or invites, or they've all expired.
No plug icon	This person has not received an activation code or invite.



Note: The clock icons are indicators of when a person last logged in. See **Monitor and Manage Remote Sessions** above for more details.

Monitor Device Status

1. In the Conductor, go to **Devices**.
2. Filter the device list, if desired.
3. In the **Device** list, look at the clock icons next to the **Overlay IP** column. The clock icon shows by color the last time the device was online. Hover over the icon to see the last time and date the device was active:

Icon	What it means
Dark Green	Currently online
Light Green	Has been online in the past

Icon	What it means
	Has never been online

For more information on the icons you might see in the Conductor and what they mean, see [Conductor Icon Reference](#) on page 36.

Update your Conductor and Airwall Edge Services

Update firmware and software, and maintain your Conductor and Airwall Edge Services.

You must be a System Administrator to apply firmware updates to the Conductor and Airwall Edge Services.

As an administrator, you deploy firmware updates to your Conductor and all Airwall Gateways from the Conductor, or you can manually update the firmware on individual Airwall Gateways using diagnostic mode.

Manage Versions of Airwall Agents and Servers

As an administrator of an Airwall secure network, you can manage which versions of software the Airwall Agents and Servers accessing your secure network use.

You do this by setting the version of Airwall Agents and Servers offered for people to install.

To set versions of Airwall Agents and Servers offered:

1. Log in to the Conductor with a system administrator account.
2. Go to **Settings**, **Advanced**.
3. Under **Global Airwall Agent Settings**, select **Edit Settings**.
4. Under **Preferred Airwall agent version**, select the version you prefer.

The version you selected is now automatically provided to people when you onboard them using **Airwall Invitations**, Activation codes, or People Groups.

Update Conductor Firmware

How to update the firmware for an Airwall Conductor.

Roles

System Administrators

Firmware downloads

 **Important:** Before you roll out a Conductor firmware update, create, download, and archive a Conductor database backup. See [Create a Conductor database backup](#) on page 412.

If your Conductor has access to Tempered's release repository on the Internet, the latest firmware downloads for your Conductor (and Airwall Edge Services) are automatically available on the Conductor **Settings** page. Otherwise, you can download the software from [Latest firmware and software](#) on page 431 and upload it to your Conductor.

Update non-HA Conductor firmware

 **CAUTION:** When you are updating firmware, stay on the page (do not navigate away or log out). If something interrupts a Conductor firmware update (for example by a power outage), it may leave the Conductor in a corrupted state.

1. Log in to the Conductor using a system administrator account.
2. Go to **Settings > General Settings > Firmware Updates**, and find the version you want.



Note: You can also download firmware from [Latest firmware and software](#) on page 431 and then upload it to the Conductor.

- For the update you want, select **Download**. The Conductor downloads the update to your Conductor.



Note: If you're uploading the firmware update, select **Upload Firmware**, select the Conductor firmware file you downloaded, and then select **Upload**. Wait on that page until the upload is complete.

- When it completes, select **Install** to install the update.

Verify the firmware version under the **Configuration** section on the **Settings** page.

Update a Conductor HA pair

When upgrading a pair of HA Conductors, the sequence in which you perform the steps below between master and standby is critical:

- Download, **but do not install**, the new firmware to the current **active** Conductor 1.
- Install the new firmware on the **standby** Conductor 2 **first**. When it finishes the update, it reboots and becomes an active Conductor.
- Install the new firmware on the now original active Conductor 1.
- Last, demote the former standby Conductor 2 to the standby role

This table shows the sequence of the update.

Step	Conductor 1	Conductor 2
1	Active Download firmware to the current active Conductor 1	Standby
2	Active Install the firmware update on Conductor 2	Standby
3	Active Install the firmware update to Conductor 1.	Active
4	Active Return Conductor 2 to the standby role.	Standby

Detailed instructions to update an HA pair

- Log in to the **active** Conductor 1 using a system administrator account.



CAUTION: During the update process, stay connected to the Conductor, and do not navigate away from the UI. Uploads and updates may take several minutes to complete. If the Conductor firmware update is interrupted (for example by a power outage), it may leave the Conductor in a corrupted state.

2. Go to **Settings > General Settings > Firmware Updates**, open the version subtab, and find the Conductor update you want to install.
3. To the right of the update, select **Download**. Stay on the page while it downloads.
4. Log out of the active Conductor, and log in to the **standby**.
5. Go to **Settings > General Settings > Firmware Updates**, and open the version subtab. The new firmware update has synced from the active Conductor and should be listed in the **Firmware Update** section.
6. On the **standby** Conductor, for the update you want, select **Install**. Stay on the page until the installation completes. After the update installs successfully, the standby Conductor reboots and becomes an active Conductor.
7. Log in to the **original active** Conductor 1, and go to **Settings > General Settings > Firmware Updates**.
8. Next to the update you want, again select **Install**. Stay on the page until the installation completes. After the update installs successfully, the Conductor 1 reboots.
9. Log back in to the **original standby** Conductor 2 and go to **Settings**. In the **Airwall Conductor high availability** section, select **Edit Settings** and then select **Demote to standby**.

Update Airwall Gateway firmware

Administrators can update the firmware for provisioned and managed Airwall Gateways directly from the Conductor. You cannot update Airwall Gateways in the factory reset state – you must provision and manage them first.

Roles

System Administrators – Download and update

Network Administrators with permissions to the Airwall Gateways – Update

You can update firmware on individual Airwall Edge Services or apply updates to groups.



CAUTION: To prevent data loss and potential corruption, it is critical that Airwall Gateways remain powered on during the firmware update process. A loss of power during the firmware update process may leave the Airwall Gateway in a corrupted state.



Note: During the update process, Airwall Gateways go offline for a few minutes as they install the firmware update and then reboot. See the current state of any Airwall Gateway on the Airwall Edge Services page.

You can also manually update Airwall Gateways not currently connected to a Conductor. For more information, refer to your model's Product Guide.

Download Airwall Edge Services firmware updates

In v2.2.8 and later, the Conductor Settings page shows a list of the Firmware updates available for your Airwall secure network, and makes it easy to download and install firmware updates.

Download firmware updates (v2.2.8 and later)

1. Log in to the Conductor with a system administrator account.
2. Go to **Settings > General Settings**.
3. Under **Firmware updates**, select **Check for Updates**. The Conductor displays the updates available for your Airwall Edge Services.
4. If you have more than one version available, select the tab for the version you want.
5. Find the firmware updates you want to apply, and select **Download** to download each update. When they finish downloading, the **Download** links change to **Install**.
6. Select **Install** and check the boxes for the Airwall Edge Services to apply it to the next time they connect to your Airwall secure network.
7. Select **Apply** to start the installation.

You can also update a group of Airwall Edge Services. For more information, see [Update firmware for a group of Airwall Edge Services](#) on page 110.

Download firmware updates (v2.2.5 and earlier)

1. Download the relevant Airwall Gateway firmware files for your Airwall Gateway models, and save them on the computer you use to access the Conductor.
2. Log in to the Conductor as a System Administrator.
3. Go to the **Settings > General Settings**, and click **Upload firmware**.
4. Select the Airwall Gateway firmware file and click **Upload**.

Update Airwall Gateway firmware

You can update the firmware for a single Airwall Gateway from the **Airwalls** page.

1. Go the **Airwalls** page.
2. For the Airwall Edge Service you want to update, open the **Actions** menu and select **Update Firmware**.
3. Select the version you want to install and then select **Apply**.

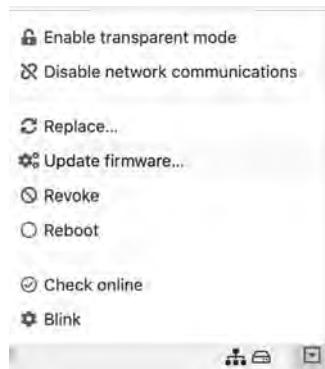


Note: If you are updating a virtual Airwall Gateway, and receive a message that the disk space is too low, see [Expand the Disk Size for a virtual Airwall Gateway](#) on page 265.

4. The installation process starts, and can take several minutes to complete.



 **Note:** The **Update firmware** option is only available if there is a current update available for that Airwall Gateway.



5. After the Airwall Gateway reboots, go to the **Airwalls** page, and verify that the new firmware version is displayed in the **Model** column.

Airwall edge services

Airwalls		
	Airwall groups	Airwall relay rules
Create group...	Airwall actions...	
Airwall	Model	Status
<input type="checkbox"/> 053D8ECAAF3B BHI@40130#053D8ECAAF3B	Airwall-Android v2.1.5	10.101.102.29
<input type="checkbox"/> 10192010007D BHI@40130#10192010007D	Airwall-100g v2.1.4	166.167.45.227
<input type="checkbox"/> 101920100080 BHI@40130#101920100080	Airwall-100g v2.2.8	10.0.0.123
<input type="checkbox"/> 101E201000CE BHI@40130#101E201000CE	Airwall-100e v2.2.8	192.168.3.132

Update firmware for a group of Airwall Edge Services

There are two ways to update firmware for multiple Airwall Edge Services at a time. One is to update using Airwall groups, and the other is to update by firmware update package.

Roles

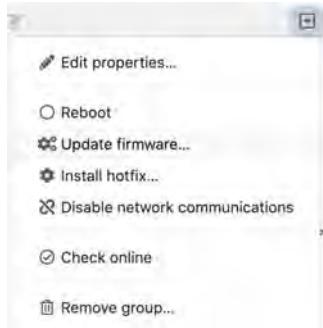
System Administrators

Network Administrators with permissions to the Airwall Gateways and Overlays

Update by Airwall group

1. Log in to the Conductor as a system administrator.
2. Open the **Airwalls** page and select **Airwall groups**.

- Find the group you want to update, and from the **Actions** menu, select **Update Firmware**. The firmware update process starts for all Airwall Edge Services in the group, and can take several minutes to complete and come back online.



- Complete the above steps for each group that requires the firmware update.
- Once complete, go to the **Airwalls** page, and verify that the new firmware version is displayed for each updated Airwall Edge Service.

Update by firmware update package

- Log in as a system administrator to the Conductor.
- Go to **Settings > General Settings**.
- If you have more than one version available, under **Firmware updates**, select the tab for the version you want.
- Find the firmware update you want to apply, and select **Download** to download the update.
- When it's finished downloading, select **Install**.
- On the **Apply Firmware Updates** page, check the box next to the Airwall Edge Services you want to update.
- Select **Apply**. The firmware update process starts for all checked Airwall Edge Services, and can take several minutes to complete and come back online.

Replace an Airwall Gateway

An Airwall Gateway that is a member of one or more overlay networks can be replaced by an unassigned Airwall Gateway (that is, it is not a member of any overlay network).

Roles

System Administrators

Network Administrators with permissions to the Airwall Gateways and Overlays

- On the **Settings** page, go to **Licensing** tab and grant provisioning requests for the new Airwall Edge Service.
- On the **Dashboard**, or the **Airwalls** page, find the Airwall Edge Service you want to replace.
- Open the drop-down to the right of the Airwall Edge Service you want to replace and select **Replace**.
- In the wizard, select the desired replacement Airwall Edge Service from the list of available replacements and click **Next**.



Note: The wizard only lists unassigned Airwall Edge Services. If the replacement is still used in any overlay networks, you need to remove it from all overlay networks before you can select it as a replacement.

5. If you are replacing an Airwall Gateway, check if your replacement Airwall Gateway meets the requirements to transfer the port configuration:
 - Must be port-compatible with the Airwall Gateway it is replacing. Airwall Gateway are port compatible if they belong to the same model group (300x, 400x, etc.) and the replacement Airwall Gateway has at least as many ports as those in use on the Airwall Gateway being replaced.
 - Must not use any ports in underlay or HA port group configurations that are used in overlay port groups on the Airwall Gateway being replaced.
 - Must use the same number or fewer underlay port groups, and all ports used in those port groups are also used as underlay ports on the Airwall Gateway being replaced.
 - Must be online.
6. **Skip to the last step if:**
 - You are not replacing an Airwall Gateway
 - You don't want to replicate the port configuration.
 - Your replacement Airwall Gateway doesn't meet the requirements to replicate the port configuration.
7. **If your replacement Airwall Gateway meets the requirements listed above and you want to replicate the port configuration:**
 - a) To transfer any static underlay IP configurations to the replacement, check **Transfer underlay IP addresses**.
 - b) If the Airwall Edge Service being replaced uses a public IP, check **Transfer public IP addresses** to transfer it to the replacement.
 - c) Initiate the port configuration transfer by selecting **Transfer port configuration**. The Conductor applies the new port configuration to the replacement Airwall Gateway.
 - d) When you see the confirmation that the transfer completed successfully, select **Next**.
8. Select **Finish** to complete the replacement.

When the replacement is complete, the new Airwall Edge Service is configured with the same overlay network membership, policy configurations, and user-specified information as the replaced Airwall Edge Service. A replacement Airwall Gateway will also have the same port configuration if it met the requirements and you chose to replicate them.

Back Up your Conductor and Airwall Edge Services

Back up your Conductor

Best practice is to back up your Conductor database on a regular basis.

1. In the Conductor, go to **Settings**, and open the **Diagnostics** tab.
2. Select **Download Database Backup**.

This backs up your Conductor database. To restore from a backup, see [Restore your Conductor from a database backup](#) on page 112.

Restore your Conductor from a database backup

If there are unexpected side effects or changes or updates to your Conductor, you can restore it from a database backup. A database backup restores everything except network configuration and SSL certificates. If you restore to the same Conductor, your network configuration and SSL certificates are maintained. If you restore to a different Conductor, it restores the database without changing the new Conductor's network and SSL configuration.

1. In the Conductor you want to restore, go to **Settings**, and open the **Diagnostics** tab.
2. Select **Restore Database Backup**.

This restores your Conductor database. To back up your database, see [Back up your Conductor](#) on page 112.

Back up Azure Airwall Gateway 300v

You can back up your Azure Airwall Gateway by taking a snapshot in the Conductor.

1. Open the Airwall Gateway that you want to take a snapshot of.
2. On the **Actions** menu, open **Cloud Operations**, and select **Snapshot**.

The screenshot shows the Conductor interface for managing an Azure Airwall gateway named 'azure'. In the top navigation bar, 'Actions' is highlighted. Below it, the 'Cloud Operations' option is selected. A red box highlights the 'Snapshot' button in the 'Actions' dropdown menu. Other options in the dropdown include 'Share', 'Delete', 'Replace...', 'Revoke', and 'Restart'.

The Conductor creates a Snapshot object in the same Azure resource group that your Airwall Gateway Virtual Machine is in.

228relayip	Public IP address	Canada Central	...
228relayNetworkSecurityGroup	Network security group	Canada Central	...
228relayProtectedNic	Network interface	Canada Central	...
228relayPublicNic	Network interface	Canada Central	...
228relayVm	Virtual machine	Canada Central	...
228relayvm-backup-200625214046	Snapshot	Canada Central	...
228relayVm_OsDisk_1_5fdd8f94788d4a1186680464fb71547d	Disk	Canada Central	...

Restore an Azure Cloud Airwall Gateway

If you've backed up your Azure Cloud Airwall Gateway by creating a snapshot, this is how you restore it.

1. Create a new Azure resource group to store the restored Cloud Airwall Gateway.
2. In that resource group, create a **Managed disk object** that uses the Snapshot from your existing Airwall Gateway as the source.

- Next to **Size**, select **Change size**, and change the **Storage type** and **Size** of the disk based on your requirements by selecting a disk size, and then selecting **Ok**.

Size	Disk tier	Provisioned IOPS	Provisioned through...	Max Share
4 GB	E1	500	50	-
8 GB	E2	500	50	-
16 GB	E3	500	50	-
32 GB	E4	500	50	-
64 GB	E6	500	50	-
128 GB	E10	500	50	-
256 GB	E15	500	50	-
512 GB	E20	500	50	-
1024 GB	E30	500	50	-
2048 GB	E40	500	50	-
4096 GB	E50	500	50	-

- Make sure the resource group and the managed disk are in the same region as the original Airwall Gateway.
- From the Azure Marketplace, start creating a new Managed Airwall Gateway.
- Select your new resource group as the destination and continue to fill out the form as you would a normal deployment.
- Rather than finalizing the deployment, on the final screen, select **Download a Template for Automation** instead.

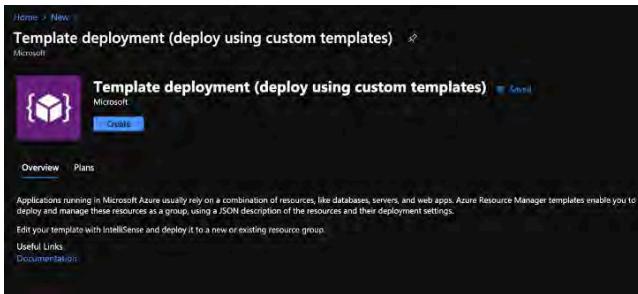
Download a template for automation

- On the next screen, click the **Download** link in the upper left. You should get a .zip file with two .json files.
- Unzip the files, and modify the template.json file as follows:
 - Remove the `osProfile` properties portion of the template.
 - Change the `storageProfile` properties to the following, filling the values for the managed disk created earlier

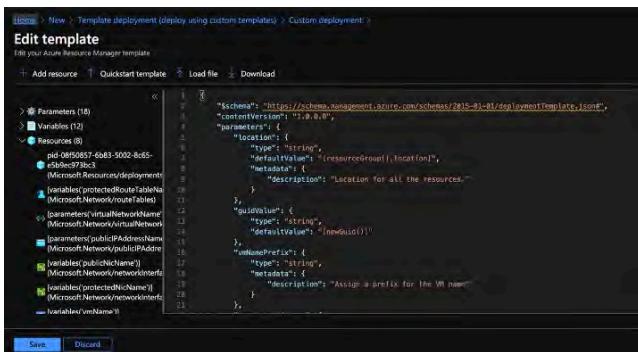
```
"storageProfile": {
  "osDisk": {
```

```
        "createOption": "attach",
        "osType": "Linux",
        "managedDisk": {
            "id": "/subscriptions/{subscription_id}/resourceGroups/
{resourcegroup_name}/providers/Microsoft.Compute/disks/
{managed_disk_name}"
        }
    }
},
```

10. Create a new Azure Template.



11. Select Build your own template in the editor, and copy the contents of template.json into the text field, and then select Save.



12. Select the **Edit parameters** at the top of the form and paste the contents of parameters.json into the displayed field and select **Save**.

The screenshot shows the 'Edit parameters' interface in the Azure portal. It displays a JSON configuration file with parameters for a VM deployment. The parameters include location ('westus'), guid ('2c670000-01e6-0000-0000-679cac0f2c27'), vmSize ('Standard_A2_v2'), vmNamePrefix ('testdemo'), vnetNewOrExisting ('existing'), and virtualNetworkName ('az-netnet'). At the bottom, there are 'Save' and 'Discard' buttons.

13. Finalize the deployment and wait for it to complete.

14. Once the restored Airwall Gateway is deployed and communicating with Conductor, open that Airwall Gateway in the Conductor, and on the **Ports** tab, update the **Underlay NAT IP** to match the new static IP object from the deployment.

The screenshot shows the 'Ports' tab in the Airwall Conductor interface for an 'Airwall gateway - azure' device. It displays port configurations for Port 1 and Port 2. Under 'Port groups', 'Underlay group 1' is selected. The 'Underlay IP (NAT)' field is set to '10.3.0.4'. Other settings shown include IP address (10.3.0.4/24), MAC (00:0d:3a:e8:c1:d9), MTU (1500), and VLAN (None). There are also sections for 'Static routes' and 'Dynamic routes'.

Conductor and Airwall Edge Service PCI Compliance

The Airwall Conductor and Airwall Edge Services are compliant with PCI DSS guidelines and Payment Card Industry (PCI) data security standards. The Airwall Solution provides secure transport of logs, firewall rules creation and reporting, retention of activity logs, and audit reporting of system configuration changes.

PCI Reporting is enabled by default. You can use it for both PCI compliance and for troubleshooting, as it records when a change was made, who made it, and what the change was.



Note: When PCI Reporting is enabled, PCI logs are kept for 90 days.

To access PCI data in the Conductor

PCI data settings are in the Conductor under **Settings > Advanced > Global Airwall settings**:

- **To enable or disable PCI reporting** – Select **Edit Settings**, and change the setting for **PCI Reporting support**.
- **To see PCI reports** – In the Global Airwall settings section, next to **PCI Reporting**, select **Downloads** to access the **PCI Report & References** download page.

PCI Compliance Reports

PCI Compliance Reports allow you to see when a change was made, who made it, and what the change was.



Note: When PCI Reporting is enabled, PCI logs are kept for 90 days.

For instructions on how to access these reports, see [Conductor and Airwall Edge Service PCI Compliance](#) on page 116.

You can download these reports from the **PCI Reports and References** page. You can cross-reference the reference ID in the User activity report with the IDs in each of the reference reports to get more details:

- **User activity report** – Contains when, what was changed, how it was changed (that is, modified, deleted, created, etc), and who changed it. Use the reference ID to look up more details in the reference reports. Includes log ins to the Conductor and authentication through an Airwall Agent or Server.
- **Policy reference** – Shows what policies are set, including the overlay the policy is in and the permissions between devices. Gives you a reference for what things on your network can connect with each other.
- **Device reference** – Details for changes on **Devices**.
- **Device group reference** – Details for changes on **Device groups**.
- **Airwall reference** – Details for changes on Airwall Edge Services.
- **Airwall group reference** – Details for changes on **Airwall groups**.
- **Overlay network reference** – Details for changes on Overlays.
- **Relay rule reference** – Details for changes on relay rules.
- **Tag reference** – Details for changes on tags.
- **User reference** – Details for changes on users.
- **People groups reference** – Details for changes on people groups.

Deploy Airwall™

Successfully deploy and configure the Airwall solution and revolutionize security on your network. This deployment information assumes you are familiar with basic networking concepts and have a good working knowledge of your organization's hardware, software, and virtual products and services.

Get Started with the Airwall Solution

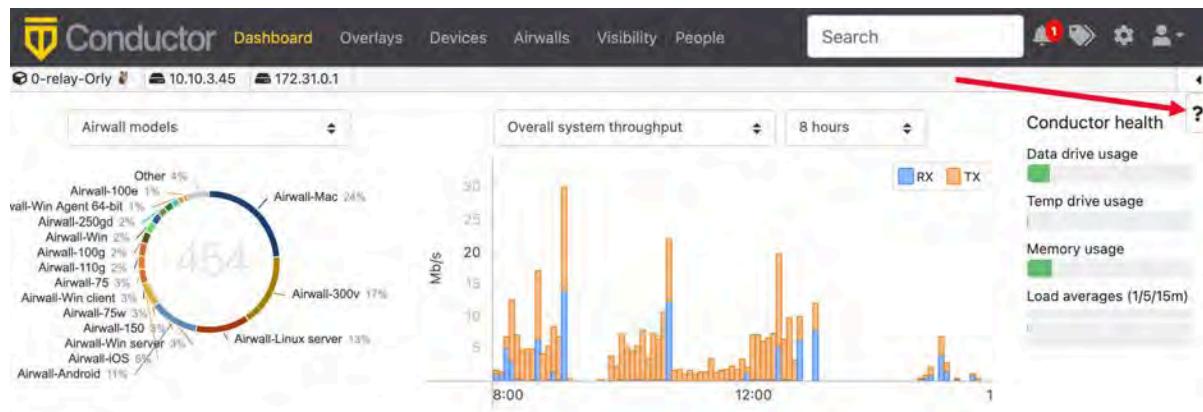
Tempered is on a mission to revolutionize security for a connected world. The Airwall Solution increases security, reduces complexity, and dynamically handles changes on your network, simplifying how you manage your network. You can instantly provision and revoke networking and security services with minimal, if any, modification to your underlying network, applications, or infrastructure. Airwall helpThis guide contains information and instructions to help you deploy, manage, and troubleshoot your Airwall Solution.

Get Started using Conductor Help and Tutorials

The Conductor contains several tutorials to help you set up and configure a new Conductor, as well as use and understand different features in the Conductor.

Open Airwall Help

Airwall Help is always available from the Conductor by going to the question mark in the upper right under the menu pane.



Use the Dashboard Setup Progress Bar

If you're a system administrator, when you first sign in to a newly-created Conductor, by default the Dashboard shows a Setup progress bar to walk you through configuring your Conductor. Select a step to get information and assistance completing that step, as well as see your progress or go back and change the configuration.

You can hide the Setup progress bar by clicking the hide icon . You can show it again from your user preferences. For help, see [Show or Hide Conductor Setup progress](#) on page 30.

Start a Tutorial

When there is a tutorial available for the page you're on, you can access it under the Conductor help icon, or from the question mark on a page.



Examples

- **People groups tutorial** – To access the tutorial on people groups, go to the **People** page, select the **People groups** tab, and then click the question mark in the upper right to see the tutorials for the **People groups** tab:

The screenshot shows the Conductor dashboard with the 'People' page selected. The 'People groups' tab is active. In the top right corner of the main content area, there is a tooltip with a question mark icon and the text 'Tutorials' and 'People group intro'. Below the main content, there is a 'Show online help' link.

- **Create a new network tutorial** – When creating a new overlay network, you can access the tutorial information by selecting the question mark icon in the lower left:

The screenshot shows the 'Create New Network' dialog box. The 'Manual network' option is selected. On the right side, there is a tooltip with a question mark icon over the 'Network topology' section, which contains descriptive text about creating an overlay network. At the bottom right of the dialog box is a yellow 'Okay' button.

Stop a Tutorial

To stop a tutorial, just select the X in the upper right corner or select **Done**.

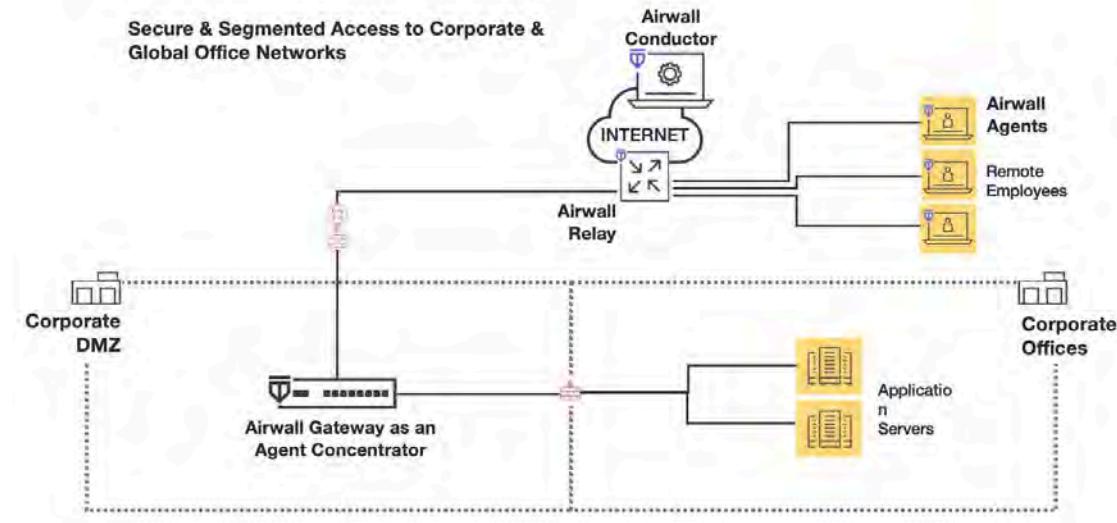
What makes up an Airwall secure network?

Get an overview of what goes into creating an Airwall secure network, a virtual air-gap solution that ensures your devices are completely invisible. You can secure and micro-segment network communication and remote access between devices at scale. The architecture also makes it possible to deploy and install an Airwall secure network over your existing network.

In an Airwall secure network, devices are assigned a cryptographic identity using Host Identity Protocol (HIP) as the sole criteria for network communications. By default, devices only communicate through the encrypted identity framework, which means devices don't even show up on a pen-test scan.

Rather than finding a metaphorical ‘locked door,’ there is no door to even knock on. From the perspective of a pen tester or bad actor, the network is essentially invisible.

Here is a simplified view of an Airwall secure network:



Airwall Agents, Servers, Gateways, and Relays, collectively Airwall Edge Services, are a collection of services that allow you to connect and protect all of your things. The Airwall Conductor provides an intuitive interface for you to manage your Airwall solution.

- Airwall Agent software protects and connects your employees mobile devices and laptops.
- Airwall Server software protects and connects your Windows and Linux servers.
- Airwall Gateways protect your devices - cameras, manufacturing, utility or hospital devices, and are available as hardware, cloud, and virtual appliances.
- Airwall Relays connect all of your things together, regardless of the way they're connecting. They route encrypted communications between all your ‘things’, without modifying the underlying network. Airwall Relays can be hardware, cloud, or virtual as well.
- The Airwall Conductor is an interface that allows you to set up and manage all of the above Airwall products and how they interact to create your Airwall secure network.
- Airwall Overlays create the connections and trust policies between these Airwall Edge Services. When you build an Overlay, you are connecting and establishing trust between two or more Airwall Edge Services.

More information on each of these is below.

Airwall Agents

Airwall Agents are software applications installed on devices (Windows, macOS, iOS, iPadOS, and Android) that enable zero-trust network access (ZTNA) from anywhere in the world. By default, all communications are encrypted end-to-end and multi-factor authenticated (MFA), enforcing a software-defined perimeter (SDP) at the distributed edge.

Easily integrate user authentication with device-based authentication, overcoming much of the complexity associated with extending directory services to include device-based trust. Explicitly allow or deny any device to securely connect to a network, and also easily segment access by defining resources that a device or group of devices can access. Devices don't have the session constraints and are not restricted by the number of concurrent client-to-resource encrypted sessions.

Airwall Servers

Airwall Servers support Windows Server and Linux, and behave much like Airwall Agents. They effectively make servers invisible and only allow communication with authenticated and authorized endpoints (ZTNA). Air-gap servers from unauthorized communication with a software-defined perimeter (SDP).

Airwall Gateways

Airwall Gateways protect ‘things’ downstream. They are deployed in front of devices or hosts that cannot protect themselves. Examples include legacy systems and machines, or when customers are unable to install an Airwall Agent or Server.

Physical Airwall Gateways, depending on the model, have built-in Ethernet, Wi-Fi, and Cellular (2G, 3G, 4G LTE modems), as well as Serial-over IP for the flexible link connectivity options. You can also deploy virtual and cloud Airwall Gateways.

Virtual Airwall Gateways use the 300v image and license. See [Virtual Airwall Edge Services](#) on page 124.

Airwall Relays

An Airwall Relay routes encrypted communications between all your ‘things’ across all of your networks. You can use them to reduce network complexity and enable complete connectivity between every endpoint. An Airwall Relay provides a private identity namespace that eliminates the need for public IP addresses and inbound firewall rules to connect devices.

Instead of Layer 3 rules, network addresses, or traditional routing protocols to securely connect and route privately addressed systems across networks, Airwall Relay relies on verifiable cryptographic identities to determine if a connection is allowed, and forwards only authenticated and encrypted traffic to authorized endpoints. You can deploy an Airwall Relay as a physical, virtual, or cloud device.

Airwall Conductor

The Conductor provides one centralized location for you to set up and manage Airwall products and create your Airwall secure network:

- Set up, provision, license, and manage all Airwall Edge Services.
- Manage the devices protected by Airwall Edge Services.
- Connect and set up trust relationship policies between the Airwall Edge Services with Overlays. You define the overlay network segments and systems that protected machines are allowed to access, as well as how they connect on the LAN, WAN, and public Internet.
- Monitor and troubleshoot your Airwall secure network.

The Conductor enforces visibility and access policy based on unchanging cryptographic machine identities, not network addresses that change and can be spoofed. It is not involved in the data that is exchanged between Airwall Edge Services and the devices they protect.

Airwall Overlays

When you build an Overlay, you are connecting and establishing trust between two or more Airwall Edge Services. Every endpoint in an Overlay knows the IP-layer state of its peers, and every peer maintains identity-based routing tables. This policy-based approach helps any edge service establish the most direct route to a resource within an Overlay.

The secured communications channels you create with an Overlay are encrypted HIP tunnels that allow trusted devices to communicate securely with each other across the network. These communication channels are controlled by the Airwall Edge Services deployed throughout the underlay and administered by the Conductor.

Underlay

This is your existing network. Airwall Edge Services (Gateways, Agents, and Servers) and the Conductor connect to the underlay over which you establish the Airwall secure network.

Airwall Gateway Hardware

Airwall Gateways provide cloaking, secure connectivity, identity-based routing, IP mobility, and micro, macro, as well as cross-boundary segmentation enforcement all within the military-grade encrypted fabric.

They enforce the Airwall Conductor provisioning, de-provisioning, and revocation of trust of any managed IP resource they protect. Airwall Gateways are currently available as hardware, virtual images for VMware ESXi and Microsoft Hyper-V, or cloud-based for Amazon Web Services, Microsoft Azure, and Google Cloud.

Airwall Gateway 75 Series



The Airwall Gateway 75 is designed for medical devices, point of sale systems, and others like building automation controls. It securely connects and protects those endpoints across all networks with little to no change to existing infrastructure. The 75's unique overlay technology rides on top of any network, even ones you don't control, eliminating the complexity, time, and cost associated with traditional networking and security methods. All protected endpoints are cloaked and segmented by the Airwall Gateway and all data encrypted so endpoints can't be discovered or accessed by unauthorized devices, eliminating the network attack surface. The 75's plug and play design makes universal connectivity and segmentation simple, fast, and cost-effective.

Airwall Gateway 100 Series



The Airwall Gateway 100 is a purpose-built industrial IoT edge gateway that makes connecting, collecting, and protecting IoT endpoints and data extremely secure and remarkably simple to deploy and manage. The 100 requires little to no change to existing infrastructure so you can rapidly join all SCADA, BACnet, and ICS endpoints to a private and segmented overlay network in minutes. The 100 eliminates the complexity associated with traditional network and security methods. All connected and protected devices are cloaked and can't be discovered or reached by unauthorized devices, eliminating the network attack surface. The 100's plug and play design, ruggedized hardware, and optional cellular modem makes universal connectivity and segmentation across all networks simple, fast, and extremely cost-effective.

Airwall Gateway 110 Series



Introducing a complete refresh for the 100-series platform, with 4x the power, more ports, and future-proof for your industrial / OT networks. Unlike the AW-100, the 110 will run all monitors, handle up to 6 HD streams, has more storage and memory (thus less bugs and scalability problems in the field).

The Airwall Gateway 110 is a purpose-built industrial IoT edge gateway that makes connecting, collecting, and protecting IoT endpoints and data extremely secure and remarkably simple to deploy and manage. The 110 requires little to no change to existing infrastructure so you can rapidly join all SCADA, BACnet, and ICS endpoints to a private and segmented overlay network in minutes. The 110 eliminates the complexity associated with traditional network and security methods. All connected and protected devices are cloaked and can't be discovered or reached by unauthorized devices, eliminating the network attack surface. The 110's plug and play design, ruggedized hardware, and optional cellular modem makes universal connectivity and segmentation across all networks simple, fast, and extremely cost-effective.

Airwall Gateway 150 Series



The Airwall Gateway 150 is a cost-effective and ruggedized Industrial IoT edge gateway that delivers peer-to-peer encrypted and segmented connectivity for machines anywhere in the world. It comes with PoE input, Serial-over-IP, and optional cellular module with seamless failover between wired and cellular networks for high availability. The 150 is often deployed as a bump-in-the-wire for machines that cannot protect themselves, while being easily managed with point-and-click policy configuration through the Conductor.

Airwall Gateway 250 Series



The Airwall Gateway 250 is a ruggedized industrial IoT edge gateway that makes connecting, collecting, and protecting ICS and SCADA systems and data extremely secure and remarkably simple to deploy and manage. Its Ethernet and SFP port dense design with PoE, dual cell modems, and link management eliminates the cost, complexity, and availability limitations of deploying separate switches, VPNs, Firewalls, Cellular Routers, and APNs.

Deployment requires little to no change to existing infrastructure, so you can rapidly join all ICS and SCADA systems to a private and segmented overlay network in minutes. The 250's unique overlay technology rides on top of any network, even ones you don't control, eliminating the complexity associated with traditional networking and security methods. All protected endpoints are cloaked and segmented by the 250 with all data encrypted so endpoints can't be discovered or data accessed by unauthorized devices, eliminating the network attack surface. The 250's plug and play design makes universal connectivity and segmentation across all networks simple, fast, and extremely cost-effective.

Airwall Gateway 400 Series

The Airwall Gateway 400 is a 1U rack mounted unified secure networking appliance. Designed to support mission-critical applications and servers throughout your organization, the 400 enables instant connectivity, cloaking, segmentation, mobility, and failover, as well as the ability to disconnect any physical or virtual resource behind it instantly. All communication from the 400 series is automatically AES 256 encrypted to any other Airwall Edge Service within the fabric and is not limited by the number of concurrent virtual trust segments that can be established.

It's the ideal choice for data center and enterprise network devices, machines or hosts that contain sensitive information, like financial servers, HR applications, 3rd party web services, or any systems with personally identifiable information (PII).

The 400 provides 8 Gigabit Ethernet ports and is configurable to meet SFP and 10G SFP+ requirements with the option to configure high availability (HA) for seamless failover between 400 Series appliances.

Airwall Gateway 500 Series



The Airwall Gateway 500 serves as a datacenter, campus, or plant services gateway that functions as either a hub or aggregation point and makes connecting, collecting, and protecting thousands of endpoints and data extremely secure and remarkably simple to deploy and manage.

The 500's high performance, port density, dual power, and optional FIPS and port expansion modules eliminate the cost, complexity, and ineffectiveness of managing VPNs, firewalls, VLANs, ACLs, and NAC for secure connectivity and segmentation across any network. The 500 serves as the network boundary and security perimeter for its protected endpoints. Its unique overlay technology rides on top of any network, even ones you don't control, eliminating the complexity associated with traditional network and security methods. All connected devices behind the 500 are cloaked and can't be discovered or reached by unauthorized devices, eliminating the network attack surface. The plug and play design makes universal connectivity and segmentation across all networks simple, fast, and extremely cost-effective.

Virtual Airwall Edge Services

The Airwall virtual Airwall Gateway is offered on multiple virtual platforms, including VMware ESXi and Microsoft Hyper-V, if you prefer a virtual form factor as a cost-effective data center implementation or a solution where a hardware-based Airwall Gateway may be impractical.

Airwall supports the following virtual platforms:

- Windows Server Hyper-V 2012 or later
- VMware ESXi version 5.0 or later

Virtual Airwall Gateways use the 300v image and license.

Cloud-Based Airwall Edge Services

Cloud Airwall Gateways are offered on multiple cloud platforms if you prefer a virtual cloud form factor as a cost-effective data center implementation or a solution where a hardware-based Airwall Gateway may be impractical.

Airwall supports the following virtual platforms:

- Alibaba Cloud – See [Alibaba Cloud – Set up an Airwall Gateway](#) on page 268.
- Amazon Web Services – See [nest_install_hipswitch_aws.ditamap](#).
- Microsoft Azure-- See [Microsoft Azure – Set up an Airwall Gateway](#) on page 277.
- Google Cloud – See [Google Cloud \(GCP\) – Set up an Airwall Gateway](#) on page 283.

Airwall Agents and Airwall Servers

Airwall Agents and Airwall Servers are designed to provide desktops, laptops, and servers with encrypted access from anywhere in the world, over any network. An Airwall Agent or Airwall Server protects the device on which it is installed.

Airwall Agents (Windows, macOS, iOS, and Android)

A Airwall Agent enables granular remote access to the network resources for employees, contractors, and vendors, without complex management of certificates, ACLs or IPSec tunnels.

Airwall Servers (Windows and Linux)

Serving as the network boundary and security perimeter for its protected workload, the Airwall Server can be deployed with little no changes to existing infrastructure and eliminates the complexity associated with traditionally separate network and security controls.

A workload protected by an Airwall Server can be cloaked and made undiscoverable by unauthorized systems. Server access is then restricted to only other authenticated and authorized Airwall Edge Services connecting from any network, significantly reducing the network attack surface.

Airwall Agents and Airwall Servers are a better alternative to virtual private networks

A virtual private network (VPN), while providing a host-to-network tunnel, lacks segmentation once authenticated and inside the network. In contrast, an Airwall Agent or Airwall Server allows secure access to mutually-authenticated and authorized machines only, making it easy to create private workgroups that are invisible and inaccessible to others, even from clients that may have valid user or application credentials. This allows devices to be logically segmented, connected, and protected in a manner that VPNs and firewalls cannot achieve.

Benefits

Universal Mobility: Instant Access and Revocation from Anywhere

Granting and revoking Airwall Agent access to individual resources on the network is simple and instant. The security context and ability to connect clients to specific resources never changes, regardless of where a user may be coming from – the LAN, WAN or Internet. The result is access from anywhere in the world, without the complexity and inflexibility of VPNs.

Airwall Invitations: Automate Rapid Deployment and Access

Automate user device access using **Airwall Invitations** to create secure and segmented access to individual resources, not entire networks. Provide email addresses, and as users download and add their machines, they'll have access to only the specific systems they're allowed and cannot see or access others, even if those systems reside on the same network. This significantly simplifies the time-consuming and complex process of getting people access to resources on the network.

Seamless and Transparent Multi-Factor Authentication (MFA)

Once the Airwall Agent is installed on a device, it now has an immutable and unique machine identity. Unlike port forwarding that enables arbitrary connections with no requirement for authentication, Airwall Agents are authenticated and authorized based on their trusted machine identity before a peer-to-peer encrypted connection is established and credentials used. User authentication can now be easily integrated with device-based authentication, overcoming much of the complexity associated with attempts to extend directory services to include device-based trust.

Private Workgroup Networks: Protect Intellectual Property and Sensitive Data

Our customers easily and quickly create overlay networks to isolate and control access to critical systems. For example, this includes controlling administrator access to network and security infrastructure to eliminate

the threat of a hacker gaining access to those systems through a system's local management interface. Another example is creating private workgroups for DevOps, Executive, HR, and PCI teams to protect intellectual property and sensitive data from being breached by unauthorized machines with access to the same network.

What's New by Version

Find out what new features have been introduced in each version.

What's New in 3.0

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and administration of an Airwall secure network.

Add Trust Policy using Drag-and-drop

You can now add and remove trust between devices on an overlay visually, or through context menus on a graph. Changes to trust on the graph are reflected on the **Devices** tab.

[Learn more – Add and remove device trust](#) on page 360

Backhaul Bypass

You can designate an Airwall Gateway as a bypass egress and then point other Airwall Gateways at it so they can reach bypass destinations through the designated bypass Airwall Gateway.

[Learn more – Backhaul Bypass](#) on page 333

Bulk Editing of People and People Groups

You can add many local users to the Conductor at one time by importing them in bulk. You export a .csv file as a template or with current users, and then import to add people to the Conductor in one step.

[Learn more –](#)

- [Import people using a CSV file](#) on page 51
- [Remove people in bulk](#) on page 53

Customized Permissions for System and Network Administrators

You can fine tune permissions for system and network administrators, giving you finer control over permissions on your network.

[Learn more – Customize Permissions for System and Network Administrators](#) on page 46

Streamlined Conductor View for Network Administrators

One of the custom permissions you can set for Network administrators provides them with a streamlined view that can simplify their workflow. Network administrators using the streamlined view can manage their overlays, and the devices, **Device groups**, and Airwall Edge Services in them.

[Learn more – Set a Streamlined View for a Network Administrator](#) on page 48

Reports

You can now run reports on different types of network activity on your Airwall secure network, including:

- Onboarding and offboarding of Airwall Edge Services or people
- Status of Airwall Edge Services or devices
- Conductor local or remote access

Learn more – [Run Network Activity Reports](#) on page 101

Monitors and Alerts

This version includes the following additions:

- **CPU Frequency** – The Airwall health data monitors can now monitor CPU frequency.
- **Details for Intrusion prevention** – Intrusion prevention alerts now indicate which devices are the source or destination of the alert where possible.

Conductor Customization

You can customize the Conductor login screen and emails sent from the Conductor for your business. Here's what you can customize:

- **Conductor login screen** – Add your company logo, and change the background colors and favicon.
- **Conductor emails** – Add your company logo and change the text color. You can also customize the subject line and add a note from the administrator when sending Airwall Invitations.

Learn more –

- [Customize the Conductor](#) on page 41
- [Customize the Conductor Login page](#) on page 41
- [Customize Conductor emails](#) on page 42

Disconnected Mode

Reduce the traffic from Airwall Agents and Servers connecting to your Conductor by setting up Disconnected mode. In Disconnected mode, Airwall Agents and Servers connect to your Conductor at intervals – between 10 minutes and 12 hours (720 minutes) – to get updates when people are not actively using the connection.

By reducing the traffic on your Conductor, Disconnected mode allows you to improve performance and scalability of your Airwall secure network. In v3.0, Disconnected mode is supported by the v3.0 Android, Linux, and macOS Airwall Agents and Servers.

Learn more –

- [Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers](#) on page 82
- [Sync an Airwall Agent or Server in Disconnected Mode](#) on page 29

Airwall Invitations

This version includes several enhancements to Airwall Invitations:

- When you're creating **People groups** with user onboarding enabled, you now have the option to send email to users when they get an activation code in the system. The email provides instructions on how to download an Airwall Agent and connect it to the Conductor.
- The email sent with Airwall Invitations has more options for customization. See **Conductor Customization** above.
- Airwall Invitations can now be used to give activation codes to existing users in addition to sending them to an email address or bulk downloading them. See the [Airwalls > New Airwall invitations](#).
- The naming schema for Airwall Invitations can now include the hostname of the connecting Airwall Edge Service.
- You can now include the hostname of the connecting Airwall Edge Service when naming devices connecting using Airwall Invitations.

Learn more – [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71

Linux Airwall Server

This version includes these additions to the Linux Airwall Server:

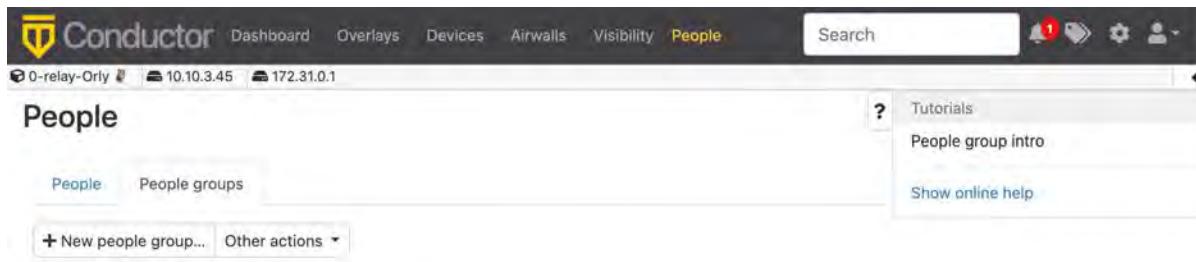
- **DockerHub deployment** – The Linux Airwall Server can now be deployed in a container from [DockerHub](#) using Ubuntu18 and CentOS8. For additional example Dockerfiles, contact Customer Success at support@tempered.io.
- **Supports Airshell** – The Linux Airwall Server now has the Airshell command-line utility. To start it, type `sudo airsh` (root user) or `sudo airwall -s`
- **Ping from port groups** – The ping function can now ping from the underlay or overlay port groups.
- **Firmware updates** – The Linux Airwall Server can now be updated from the Conductor.

Learn more –

- [Connect with a Linux Airwall Server](#) on page 26
- [Linux Airwall Server Airshell commands](#) on page 309

Conductor Tutorials and Help

The Conductor now contains several tutorials to help you set up and configure a new Conductor, as well as use and understand different features in the Conductor. You can also directly access Airwall help from the Conductor:



Learn more –

- [Get Started using Conductor Help and Tutorials](#) on page 118
- [Show or Hide Conductor Setup progress](#) on page 30

Licensing Updates

In v3.0, the following licenses have been changed:

- The Airwall Gateway 100V is no longer available
- You no longer need a separate license for port mirroring

Manage failover between underlay port groups

The Link Manager that Conductor uses to manage port failover groups has been improved. The following has been updated:

- You can now set port group link auto-repair globally per Airwall Gateway.
- You can now manage underlay links independently by traffic type.
- When you set up link failover groups, you can now require all pings to be successful if multiple ping destinations are assigned.

Learn more – [Manage Failover between Underlay Port Groups](#) on page 326

API Updates

The following updates and improvements have been made to the API:

- **Pagination** is turned on by default in 3.0 for all index endpoints, which may affect existing scripts. Enabling pagination helps scale Conductor capacity. If you need to preserve existing behavior, add a query parameter for `pagination=false` to any index API endpoints you are using.
- The API for **Airwall Invitations** now includes new invitation methods: email invites, download multiple activation codes, apply an invite to an existing person, or download a reusable invitation. The documentation has also been updated.

- **People reference** now includes `person_group_ids` and `overlay_network_ids`.
- **Person groups reference** now includes user onboarding configuration information.

Terraform Deployment Support

This version contains Terraform deployment support for Conductors, Airwall Gateways, and Linux Airwall Servers for all supported Cloud Providers. For example plans, please contact Customer Success at support@tempered.io.

New and Improved Conductor Features

Dashboard

The Dashboard now includes a **Provisioning** tab where you can see and manage all provisioning requests.

General

There is now infinite scrolling for lists on most pages, and streamlined inline editing, including direct editing of names and tags at the top on most pages.

Devices page

This page has been simplified, and provides more details on device conflicts to help you troubleshoot.

People page

Administrators can now view the Airwalls owned by a person from the person details page.

Settings

The Conductor Settings page has been streamlined and reorganized to make it easier to find the settings you want.

New Airwall Agent user authentication settings

New settings allow you to automate assigning an Airwall Agent owner: **Require owner for Airwall Agent authorization** and **Auto-assign Airwall agent owner on login**.

Replacing Airwalls

You now have the option to revoke, or both revoke and delete, a source Airwall Edge Service after replacing. Replaced Airwall Edge Services that are not deleted are named "<old name (Replaced by UID of replacement)>" to make them easier to find.

Diagnostic Tools on the Standby Conductor

You can now use diagnostic tools on a Standby Conductor.

Better CA certificate replacement and removal handling

When you replace your CA certificates, any Airwall Gateways with custom certs installed now check their cert against the new CA. If they cannot be verified, the cert is removed so the Airwall Gateway does not lose access to the Conductor. If the CA is removed entirely, all customer certs are also removed.

Learn more –

- [The Conductor Dashboard](#) on page 32
- [Configure Authentication Options](#) on page 203

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- [Expand the Disk Size for a virtual Airwall Gateway](#) on page 265

- [Airwall Gateway 75 Installation Guide \(PDF\)](#)

Updated –

- [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71
- [Configure Port Groups with Airshell](#) on page 312
- [Set up Conductor high availability](#) on page 231
- [Manage devices dynamically with Smart Device Groups](#) on page 87
- [Configure a Conductor IP, Friendly URL, or Port](#) on page 198
- [Understand People Roles and Permissions](#) on page 49
- [Configure Conductor Remote Logging](#) on page 236
- [Enable DNS lookup for bypass destinations](#) on page 336
- [Monitor Activity and Connections](#) on page 100
- [Integrate Third-party Authentication with OpenID Connect](#) on page 208
- [Airwall Gateway Airshell Console Commands - airsh](#) - New conf model command

What's New in 2.2.13

Here are the new features and enhancements in this version.

Advantech Airwall Gateway

You can now use an Advantech ICR-32xx model router and install Airwall Gateway AV3200g firmware on it. The Advantech is a rugged form factor that you can install in harsher environments. The Advantech Airwall Gateway firmware supports Ethernet and Cell, as well as Serial port access and Serial over IP. It does not currently support Wifi or the second SIM socket. You must upgrade your Conductor to 2.2.13 to use the Advantech Airwall Gateway. If you're interested in this option, please contact Customer Success at support@tempered.io.

[Learn more – Set up Advantech hardware](#) on page 243

New and Improved Conductor Features

Port mirroring

Airwall Gateways configured with port mirroring now show mirrored status in list and status views.



DEV-15399

OpenID Connect

OpenID Connect tokens are now included in the webapp log at the debug level to assist with integration.

User Preferences

The Conductor now remembers user page size settings across sessions, browsers, and computers.

Underlay Network view

This view now visually separates the different underlay IPs to show their ping statuses, RTT, and count as they are being pinged.

Device name now shown on Overlay and Device pages

If you set a name for a device in an Airwall Agent or Server, it is now shown on the **Overlays** and **Devices** pages in the Conductor.

CPU Graph Changes

Starting with 2.2.12, the CPU graph on an Airwall Gateway Reporting page now shows CPU percentage, not the previously-shown CPU load average. The CPU percentage graph shows the percentage of CPU capacity being used on the Airwall Gateway over time.

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- [Diagrams for Port Mirroring](#)
- [Virtual Airwall Edge Services](#)

Updated –

- [How Airwall Licensing Works](#) on page 159
- [Set up a virtual Airwall Gateway in VMware ESX/ESXi](#) on page 259
- [Set up a virtual Airwall Gateway in Microsoft Hyper-V](#) on page 261
- [Alibaba Cloud – Set up an Airwall Gateway](#) on page 268
- [Amazon Web Services – Set up an Airwall Gateway](#) on page 273
- [Microsoft Azure – Set up an Airwall Gateway](#) on page 277
- [Google Cloud \(GCP\) – Set up an Airwall Gateway](#) on page 283
- [Airwall Gateway Airshell Console Commands - airsh](#) - New conf model command
- [Mirror Traffic to a Dedicated Port](#)

What's New in 2.2.12

Here are the new features and enhancements in this version.

Licensing Changes

- Port mirroring now requires an add-on license for any Airwall Gateway acting as a Mirror Source
- Licensing page changes:
 - Licenses are now paginated as needed.
 - Vouchers are automatically consolidated

Airwall Servers for Raspbian and Ubuntu ARM64

You can now get an Airwall Server that runs on Raspbian or Ubuntu ARM. For installation information, see [Raspbian and RPi4/Ubuntu ARM64 – Install the Airwall Server](#) on page 11.

Platform End of Life for 100 Series Appliances

Tempered announces the End of Life schedule for the HIPswitch 100 series platforms. For more information and a schedule, see [Platform end-of-life for Airwall Gateway/ HIPswitch 100 series](#) on page 423.

New and Improved Conductor Features

Port mirroring

Airwall Gateways configured with port mirroring now show mirrored status in list and status views.



DEV-15399

OpenID Connect

OpenID Connect tokens are now included in the webapp log at the debug level to assist with integration.

User Preferences

The Conductor now remembers user page size settings across sessions, browsers, and computers.

Underlay Network view

This view now visually separates the different underlay IPs to show their ping statuses, RTT, and count as they are being pinged.

Device name now shown on Overlay and Device pages

If you set a name for a device in an Airwall Agent or Server, it is now shown on the **Overlays** and **Devices** pages in the Conductor.

CPU Graph Changes

Starting with 2.2.12, the CPU graph on an Airwall Gateway Reporting page now shows CPU percentage, not the previously-shown CPU load average. The CPU percentage graph shows the percentage of CPU capacity being used on the Airwall Gateway over time.

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- [Diagrams for Port Mirroring](#)
- [Virtual Airwall Edge Services](#)

Updated –

- [How Airwall Licensing Works](#) on page 159
- [Set up a virtual Airwall Gateway in VMware ESX/ESXi](#) on page 259
- [Set up a virtual Airwall Gateway in Microsoft Hyper-V](#) on page 261
- [Alibaba Cloud – Set up an Airwall Gateway](#) on page 268
- [Amazon Web Services – Set up an Airwall Gateway](#) on page 273
- [Microsoft Azure – Set up an Airwall Gateway](#) on page 277
- [Google Cloud \(GCP\) – Set up an Airwall Gateway](#) on page 283
- [Airwall Gateway Airshell Console Commands - airsh - New conf model command](#)
- [Mirror Traffic to a Dedicated Port](#)

What's New in 2.2.11

Here are the new features and enhancements in this version.

Mirror network traffic for Packet Analyzers

You can now mirror network traffic to packet analyzer/visibility tools (like Nozomi or Wireshark) to see what's going on in your Airwall secure network.

See more: [Mirror traffic from your Airwall Gateways to a packet analyzer tool](#) on page 389

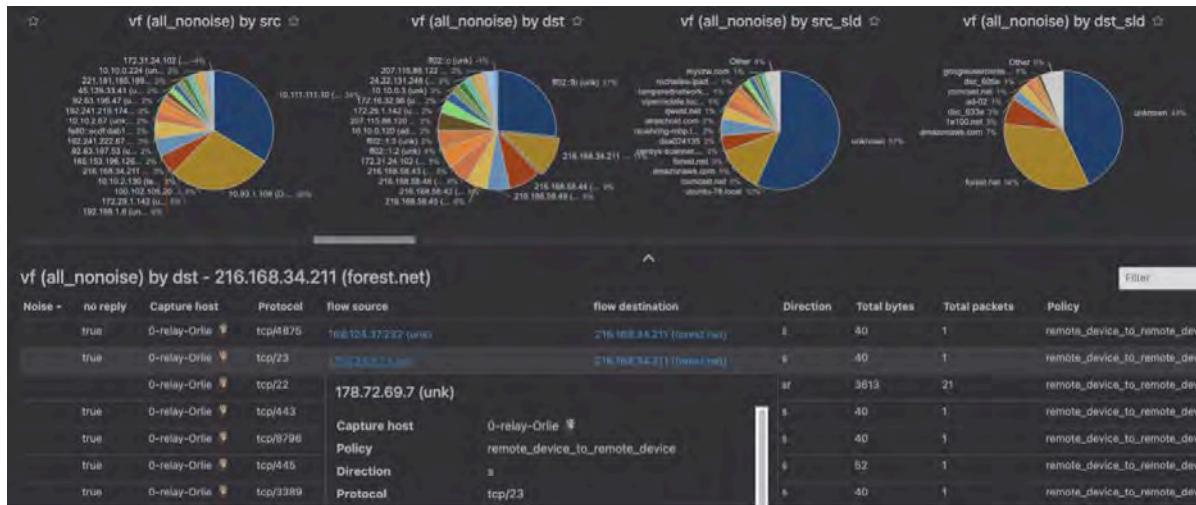
Assign Separate DNS Servers to Airwall Agents and Servers

If you need Airwall Agents and Servers to use different DNS servers, you can assign different DNS servers on an Overlay or individually for Airwall Agents and Servers that support it.

See more: [Assign Separate DNS Servers to Airwall Agents and Servers](#) on page 296

Preview - Airwall Visibility Connector

The Airwall Visibility Connector gives you a dynamic L4 view into the health and status of your Airwall secure network. You can explore many pre-computed reports in the Conductor, and can integrate other threat detection platforms. When configured, the Conductor continuously learns from these external systems, and can report or respond to threats as they are detected.



Contact Customer Success at support@tempered.io if you would like to preview this feature. A future version will expose the full feature with appropriate documentation, training, and platform options.

Raspberry Pi Airwall Agent

You can now get an Airwall Agent that runs on Raspberry Pi. For information, see .

Platform End of Life for 100 Series Appliances

Tempered announces the End of Life schedule for the HIPswitch 100 series platforms. For more information and a schedule, see [Platform end-of-life for Airwall Gateway/ HIPswitch 100 series](#) on page 423.

New Knowledge Base and Support Site

Tempered has a new site for our product Knowledge Base articles and support. Update your links!

- New Link to open a Support ticket: <https://www.tempered.io/support/supportReq.html>
- New location for Knowledge Base articles: <https://tempered.force.com/TemperedSupportCenter/s/>

New and Improved Conductor Features

Update macOS Airwall Agents from the Conductor

In v2.2.11, the macOS Airwall Agent introduces the ability to update from a Conductor package. For those running v2.2.10, upgrade one last time manually, with:

```
sudo installer -pkg /path/to/
Airwall-Mac_2.2.11.xxxx.pkg -
target /
```

You can then update future versions from a Conductor update package.

DEV-14804

Clear Recent events on the Dashboard

On the Dashboard System navigation, you can clear all events by selecting the Dismiss events icon .

DEV-15157

Recent events

New Airwall online 1710250K0182 Airwall-250gd View Manage	New provisioning request 7A9B8E687739 Airwall-300v View	New provisioning request 138BE3353252 Airwall-300v View	New provisioning request D8C1E0989CE2 airwall-linux-0cfbaeef Airwall-Linux View
--	--	--	---

New Notes field on Airwall Edge Service pages

There is now a place where administrators can add notes on Airwall Edge Service pages: DEV-15111

Airwall gateway - 10192010007D

The screenshot shows the 'Airwall gateway' configuration page. At the top, there are tabs: Airwall gateway, Local devices, Ports, Reporting, and Diagnostics. Below the tabs, there are several sections with configuration options:

- Status:** Enabled (green button)
- Member of:** Overlay networks (None), Airwall groups (& HSG-all-non-relay), Airwall relay rules (0-all-to-all)
- Online status:** 166.167.45.227
- Published IPs:** 166.167.45.227
- Tags:** Name, Location, Description, Notes

Conductor theme now follows you

Your Conductor theme is now saved across computers and browsers. DEV-15022

Failover groups improvement

Failover groups now start with an initial likely selection for underlay link failover configuration. DEV-14900

OpenID Connect improvement

OpenID Connect now supports Azure Active Directory (AD). DEV-14864

Conductor Certificate Expiration reminders

When a Conductor certificate is near expiration (1 month + 1 week), you get an event and a tag on the cert info that warns you of the upcoming expiration. On the day of expiration, you get an alert, event, and a tag telling you the certificate has expired. DEV-15160

Download a CSV with Licensing and Airwall Data

You can download all licensing and Airwall data in CSV format from **Settings > Licensing**. This data can be helpful in ensuring your Conductor vouchers are correctly renewed. DEV-14869

Access Windows Date Selection improvements

The way you choose dates for Access windows has been improved. DEV-14649

Airshell Improvements

You can now save your network configuration when doing a factory reset using the keep-networking option. See [Airwall Gateway Airshell console commands – airsh](#) on page 305. DEV-14465

Alert Improvements

Intrusion prevention alerts now indicate which devices are the source or destination of the alert where possible. These alerts are in Conductor alerts and indicated by the ID in the event data from the API DEV-14502, and snort metadata will be included in the API. DEV-14490

Diagnostic Mode Improvements

- Diagnostic Report Addition – The Diagnostic report now includes policy-based routing rules and IPv6 routes. DEV-14720
- Return to Diag mode after a hotfix – When applying a hotfix that does not require reboot, when the hotfix

is complete you get an option to return to Diag mode.

DEV-14582

API Improvements

- API tracks when changes happened – The Conductor API now serializes when many resources were created and updated, and includes These changes make it easier to see when resources were added or have changed from the API. DEV-14962
- New API endpoints – New API endpoints show history of Airwall Edge Services being managed and revoked DEV-15113, and returns a list of devices that each device has policy to and what overlays the policies are in DEV-14717.
- Date time/NTP settings – The API now allows updating of Date time/NTP settings. DEV-14716

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- [Configure an Underlay Port Failover Group](#)
- [Best Practices for Underlay Port Failover Groups](#)

Updated –

- [Seamless Bypass](#)

Introducing our new free offering – Airwall Teams

Airwall Teams allows you to build truly private system-to-system networks—that span public, private, cloud, and mobile networks using an intuitive graphical interface - just draw lines between devices you want to connect. Airwall Teams replaces and expands on our Airnet platform.

See more:

- [Sign up – Airwall Teams](#)
- [Check out the help – Airwall Teams Help](#)

What's New in 2.2.10

Version 2.2.10 of our product includes many new features and enhancements.

What's New

Access Windows for authenticated users

Specify or restrict what days and times authenticated users can log in to access resources on your secure network using Access Windows.

See more: [Set Times Authenticated Users can Access the Secure Network on page 78](#)

Automatic Relay Rules

Enable all connections in an overlay network to use a group of relays. This provides a less-granular, but simple way to manage relay rules.

See more: [Set an Overlay to Automatically Manage Relay Rules on page 82](#)

Airwall Gateway Custom Certificates

By default, Airwall Gateways come with a Tempered factory-installed certificate. You can now add your own custom CA certificate to use for Conductor communication.

See more: [Add or Replace a Signed Certificate on an Airwall Gateway for Conductor Communication](#) on page 319

Bulk Configuration of Airwall Gateways

Configure certain settings in bulk for Airwall Gateways or Airwall Gateway groups.

See more: [Bulk Configuration of Airwall Edge Services](#) on page 314

Enable DNS for Seamless Bypass

You can now enable DNS to use fully-qualified domain names (FQDN) for bypass destinations.

See more:

- [Enable DNS lookup for bypass destinations](#) on page 336
- [Seamless Bypass](#) on page 329

Setup Wizards for configuring Conductors and Airwall Gateways

2.2.10 has added two wizards to help you in deploying an Airwall secure network. The Conductor Deployment Wizard walks you through setting up, licensing, and provisioning a new Conductor, and the new Airshell (`airsh`) command `setup-ui` walks you through the most common Airwall Gateway setup options.

See more:

- [Conductor Configuration Wizard Settings](#) on page 165
- [Configure an Airwall Gateway with the airsh Setup Wizard](#) on page 237

Airwall Status Indicators

There are new ways to see information and status on the Airwall Edge Services connecting to your Airwall secure network

See more: [See Airwall Edge Service Information and Status](#) on page 98

Cloud Improvements

This release includes improvements that make it easier to deploy cloud Conductors and Airwall Gateways, and includes support for AWS GovCloud (see below):

- **ENa and SR-IOV support** – You can now deploy instances with enhanced networking configuration enabled with either ENa or SR-IOV, and see which machine types support or require ENa. Note that machine types marked as ENa may deploy as SR-IOV.
- **Disk IO has been improved** – Cloud deployments now include NVMe (memory) disk options.
- **Cloud HA deployment has been automated** – Simplified deployment for HA, eliminating many of the places where misconfiguration could happen.
- **New Azure cloud image names** – Image names now reflect their use, making it easier to choose the correct image.
- **Additional information as images are created** – More details are included in the status pane as the Conductor creates cloud images.
- **Can now choose resource groups** – You can now choose a new or existing resource group when you create cloud Airwall Gateways and Conductors.

Note: If you choose an existing resource group, make sure no resource names in the existing resource group conflict with the new Airwall Gateway and Conductor deployment name that you are creating.

- **More information available in the Conductor** – New attributes are shown for cloud Airwall Gateways on the Diagnostics tab.

Preliminary IPv6 Support

If you have devices with IPv6 addresses, IPv6 is now supported for Airwall Gateways and Linux Airwall Servers. The control for source NAT is shared for both IPv4 and IPv6. Configurations sourcing NAT IPv4 but not IPv6 are not supported.

Airwall Gateways now support static IPv6 addresses for both the underlay and overlay (some cellular carriers may not support it). You also need to assign a static IPv6 address to the Airwall Gateway.

Since IPv6 only supports routed configurations, you need to assign an IPv6 overlay address to the Airwall Gateway to use IPv6 overlay. L2/subnet extensions are not supported.

See more: [Set up a secure IPv6 overlay](#) on page 316

AWS GovCloud Support

Cloud Conductors and Airwall Gateways can be now be deployed in AWS GovCloud. Follow the instructions for deploying in AWS:

- [Deploy a Conductor on Amazon Web Services \(AWS\)](#) on page 174
- [Set up Cloud Providers](#) on page 364
- [Deploy a cloud Airwall Server](#) on page 299

Exponential Backoff

Added exponential backoff to the Airwall Gateway to/from Conductor management connection to comply with Verizon data retry requirements. This change means it could take up to 3 minutes to reconnect after an extended outage. (*DEV-14648*)

What's New in 2.2.8

Version 2.2.8 of our product includes many new features and enhancements.

What's New

New Airwall Gateway Hardware – the Airwall-110

The Airwall-110 Series is a major upgrade for the 100-Series, with higher performance and global cellular connectivity – all in a smaller form factor that maximizes the v2.2.8 improvements. The Airwall-110 has more (4x) bandwidth performance and two serial ports, runs all Snort intrusion detection monitors, handles up to 6 HD video streams, and has more storage and memory (so it has higher capacity, quality, and scalability for production environments).

See more: [Airwall Gateway 110 Series](#) on page 122

New cellular modem support

Version 2.2.8 supports the upcoming North America and Global cellular expansion trays for our Airwall-150 appliance. These LTE Category 4 expansion modules come in two variants supporting North America and Rest of World. These expansion trays allow you to connect your Airwall 150 to more cellular carriers in more countries including the United States, Canada, Australia, New Zealand, Japan, the European Union, and other countries recognizing CE RED certificates.

Conductor Dashboard and Usability Improvements

The Conductor Dashboard has been improved to give you a broader look into the status of your Airwall secure network. New features include:

- Ability to pin pages you visit frequently
- See how many Airwall Edge Services are online, and how many authenticated users are logged in.
- Easily manage new provisioning requests
- See when new firmware and software is available, and easily update your network.
- Improved user onboarding workflow (see Improved User Management below)

See more:

- [The Conductor Dashboard](#) on page 32
- [Create or Manage Dashboard Messages](#) on page 39
- [Conductor Icon Reference](#) on page 36
- [Monitor Connections to your Airwall secure network](#) on page 104
- [Download Airwall Edge Services firmware updates](#) on page 108
- [Update firmware for a group of Airwall Edge Services](#) on page 110

Improved User Management and Remote Access User Features

Remote access user management has been expanded to scale for large organizations, with the Conductor doing most of the work that admins used to have to do to invite, onboard (especially installing and activating the Airwall Agents), orchestrate, and authenticate remote access users. Onboarded users can see what they can access through the overlay networks in Conductor, eliminating frequent support calls to Conductor admins for help getting server IP addresses.

See more:

Conductor Admin Topics

- [Connect People's Devices to your Airwall secure network](#) on page 54
- [Connect People as Remote Access Users](#) on page 61
- [Connect People's Devices with Activation Codes](#) on page 63
- [Set up a People Group](#) on page 74
- [Manage Versions of Airwall Agents and Servers](#) on page 106
- [Provision Airwall Gateways using Activation Codes](#) on page 161
- [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71

End user topics

- [Change my Conductor password](#) on page 30
- [I have an Activation Code](#) on page 14
- [I want to request to connect](#) on page 17
- [I have a "Finish Setting up my account" email](#) on page 14
- [Create or Edit Airwall Agent or Server Profiles](#) on page 29
- [I'm having trouble connecting](#) on page 31

Enhanced Monitoring

You can now set monitor thresholds on health data and traffic stats to detect potential problems before they occur. We have redline stats for performance metrics of the Airwall Gateway, and for volumetric traffic stats.

Seamless Bypass (split tunnel)

Seamless bypass enables you to deploy without knowing all of the hosts to allow in an overlay policy. Seamless bypass replaces the need to create policy exceptions, and reduces the complexity, extra hardware, extra cabling, and reliance on configuration of your underlay infrastructure.

See more: [Seamless Bypass](#) on page 329

Alibaba Cloud Conductor and Airwall Gateways

You can now use Alibaba Cloud to deploy cloud Conductors and Airwall Gateways, and seamlessly connect cloud Conductors and Airwall Gateways with each other, as well as virtual and on-premises or physical environments. You can deploy an Airwall secure network on all of the major cloud providers.

See more:

- [Deploy a Conductor on Alibaba Cloud](#) on page 171
- [Alibaba Cloud – Set up an Airwall Gateway](#) on page 268

Routed Port Group Improvements

The ability to configure port groups can give you up to a 30% performance increase for common deployment cases using a single interface in the overlay port group (for example, cloud gateways, virtual gateways, and optionally on physical gateways). It is simpler to deploy and avoids multicast/broadcast chatter over the tunnel.

See more:

- [Set up Port Groups on an Airwall Gateway](#) on page 321
- [Set up an Underlay Port Group](#) on page 324
- [Set up Overlay Port Groups](#) on page 321

Custom signed Certificate Improvements

You can replace a signed certificate on the Conductor with the old certificate remaining active until the new certificate is activated.

See more: [Add or Replace a Signed Certificate for the Conductor UI](#) on page 201

Easier Deployment of High Availability Cloud Conductors

The Airwall Solution has automated the process of creating high availability Conductors in the cloud across different providers. You can now back up your Conductor and easily create an HA standby in the cloud using the Conductor's automated process and be guaranteed a successful cloud HA deployment.

See more: [Automatically Create an Standby HA Conductor in the Cloud](#) on page 228

Remote Airshell Access into Airwall Gateways

You can securely log in to the overlay IP address of an Airwall Gateway with key-based SSH, and run Airshell (airsh) commands remotely. Airsh has been enhanced to perform many of the functions of diagnostic mode. Remote access can help avoid in-person visits to perform diagnostics and troubleshooting. Status and statistics are available using airsh, which includes tab-completion and inline help.

See more:

- [Set up Remote Access to Airshell](#) on page 310
- [Access an Airwall Gateway Remotely](#) on page 311

Port configuration replication

You can now replicate the port configuration between two Airwall Gateways when setting up an Airwall Gateway HA pairing, or when replacing an Airwall Gateway.

See more:

- [Configure High Availability Airwall Gateways \(v2.2.8 and later\)](#) on page 337
- [Replace an Airwall Gateway](#) on page 111

Device Manufacturer (MAC address OUI) is now displayed

The **Devices** list now shows the manufacturer's name determined from the MAC address OUI (organizationally unique identifier), where available, in the **OUI** column. You can also now update the OUI list as needed.

See more:

- [Update the MAC address \(OUI\) \(Manufacturer\) List](#) on page 413
- [See MAC address OUI \(Manufacturer\) Information for Devices](#) on page 97
- [Search for or Sort Devices by MAC Address OUI \(Manufacturer\) Name](#) on page 97

Manage Airwall Agents through an MDM

Some MDM solutions now support managing Airwall Agents.

See more: [Manage Airwall Agents through an MDM \(Mobile Device Management\) solution](#) on page 70.

SD-WAN

An option was added to expose the Differentiated Services Code Point (DSCP) field of the inner IP header (plaintext) to the outer (encrypted) encapsulating header. This allows for classification of different types of network traffic for routing and prioritization purposes.

What's New in 2.2.5

Version 2.2.5 of our product includes many new features and enhancements.

What's New

Support for NAT Subnet Broadcasts

The Airwall Solution now supports NATing subnet broadcasts on the device network.

New Airwall help content

- [Airwall Invitations](#)
- [Renew Expired Licenses](#)
- [Integrate Third-party Authentication with OpenID Connect](#)
- [Set up an Airwall Gateway in Microsoft Azure](#)

Updated Airwall help content

- [Configure a DHCP relay on an Airwall Gateway](#)
- [Configure protected devices with DHCP](#)
- [Route encrypted connections with Airwall Relay](#)
- [Configure Airwall Relay rules](#)
- [Install Airwall Server on Linux](#)

What's New in 2.2.3

Version 2.2.3 of our product includes many new features and enhancements.

Introducing Tempered Airwall

Tempered's fully encrypted, virtual air-gap network security solution is now called Airwall. Our product offerings are also changing to match our brand and make their functions clearer.

What's New

OpenID Connect support for Airwall Clients

We have added OpenID Connect support for authenticating remote sessions on Android, iOS and macOS Airwall Agents (formerly Android, iOS, and OSx

People groups as Overlay members/managers

HIPclients). There is also now a global option to lock out clients that do not support user auth.

Lockdown Mode

People Groups are now able to be members of Overlay Networks as well as Managers of Overlay Networks. Now user permissions can be configured entirely in an authentication provider such as LDAP or OpenID Connect via people group membership.

Cloud Linux Airwall Servers

Lockdown Mode is now configurable from the Airwall Conductor for Airwall Agents (formerly HIPclients) that support this feature (currently supported by the Windows Airwall Agent).

The Airwall Conductor can create and deploy Linux Airwall Servers directly in any cloud provider, such as Azure, AWS, or Google.

New Airwall Names

Here's a translation from what we used to call things to what we're calling them in Airwall to help with the transition:

What it used to be	Airwall name
Conductor	-> Airwall Conductor
HIPservice	-> Airwall Edge Service
HIPswitch	-> Airwall Gateway
HIPclient	-> Airwall Agent
HIPserver	-> Airwall Server
HIPapp	-> Airwall Agent or Server
HIPrelay	-> Airwall Relay
hipsh	-> airsh
Tempered Networks	-> Tempered
Tempered Networks Technical Documentation	Airwall Help

You may see both old and new terms used in content and the Airwall Conductor as this transition is made.

Introducing Tempered Airwall

Tempered's fully encrypted, virtual air-gap network security solution is now called Airwall™ – a revolution in secure networking, making networks invisible. The products and parts that make up the Airwall are also changing to match and make their functions clearer.

New Airwall Names

Here's a translation from what we used to call things to what we're calling them in Airwall to help with the transition:

What it used to be	Airwall name
Conductor	-> Airwall Conductor
HIPservice	-> Airwall Edge Service
HIPswitch	-> Airwall Gateway
HIPclient	-> Airwall Agent
HIPserver	-> Airwall Server
HIPapp	-> Airwall Agent or Server

What it used to be		Airwall name
HIPrelay	->	Airwall Relay
hipsh	->	airsh
Tempered Networks	->	Tempered
Tempered Networks Technical Documentation		Airwall Help

You may see both old and new terms used in content and the Airwall Conductor as this transition is made.

Technical Documentation

If you're missing the previous Tempered Networks Technical Documentation, it's still available! All of the content for *current versions* is included and being improved right here in the new Airwall Help. If you want still want to see the pre-Airwall help, click the link on the [Airwall Help](#) home page.

What's Not Changing

What's not changing is our mission to revolutionize security for a connected world. Airwall increases security, reduces complexity, and dynamically handles changes on your network.

What's New in 2.2

Version 2.2 of our product includes many new features and enhancements.

2.2.1 HIP tunnelMonitoring

New in this release is the ability to monitor HIP tunnel state changes directly. You can configure a monitor to watch the HIP tunnel to a particular remote Airwall Edge Service or to all trusted peer Airwall Edge Services. As with all monitors, you can create actions on events to alert, change policies, etc.

2.2.1 HIP tunnelstats graph

The tunnel stats introduced in 2.1.5 for Airwall Relays is now available for all Airwall Edge Services. You can see Tx and Rx bits between any pair of Airwall Gateways, allowing you to troubleshoot underlay and overlay connectivity issues.

2.2.1 OpenID Connect

Conductors now support OpenID Connect as an external authentication provider type. You can now use an Identity and Access Management tool such as Okta or OneLogin and integrate Single Sign-On (SSO) or Multi-Factor Authentication (MFA) support.

2.2.1 Multiple Underlay Networks

We now support active/standby multi-homed wired and wireless uplinks, even allowing communication between different ISPs. Multiple Underlay Networks give you more control over which link handles HIP tunnels and which link handles connection to the Conductor.

2.2.1 Multiple Overlay Networks

We now support isolation between port groups. Each overlay port group has its own overlay IP, static routes, and related network settings. Each overlay port group bridges its interfaces, but communication between port groups requires policy.

2.2.1 Port group Configuration

The **AirwallsPorts** user interface has been completely overhauled to enable the configuration of multiple underlay and overlay port groups. Several things that were configured in different places in 2.1.x are now consolidated in one location:

- Port group
- Port role
- Failover group settings
- Wi-Fi
- Cellular
- 802.1q VLAN tags
- Overlay IP/Netmask

Interfaces appear on the screen with live status information from the Airwall Edge Service. Also, all configurations are committed only after the Airwall Edge Services validates and successfully implements the changes, eliminating disagreement between what is configured in the Conductor and what is actually implemented in the Airwall Edge Service.

2.2.1 Network Objects

You can now use a CIDR (like 10.3.5.0/24) instead of a /32 for a device address. The term **Network Objects** simply refers to a device that uses a CIDR, and this device can be used wherever you would use any other device, like in device groups and overlay networks. Using network objects, you can allowlist an entire IP network in one click. This should make policy migration from Firewalls and Routers during new deployments much easier. Site-to-site VPN becomes trivial. More specific policies are still supported, so you can create wide policies to open general site-to-site traffic and still segment traffic to Airwall Edge Services.

Negative policies are also supported so you can allow networks or individual IP addresses (like a router) and then create exceptions using a negative policy (like a firewall).

This makes it much easier to manage Airwall Edge Services. Configurations become simpler, shorter, and easier to maintain. For cloud-based Airwall Edge Services, route injection is much simpler because routes are summarized.

2.2.1 User Auth (Windows, Mac, Android; iOS to release shortly)

MacOS and Android now support the user authentication feature introduced in 2.1.3 Windows clients and Airwall Servers. macOS will support this feature in a later release. This feature allows an admin to require client users to provide an additional factor of authentication, currently username and password, to access the overlay for a period of time. Since usernames and passwords are centrally managed, this mitigates concerns about stolen laptops or devices, giving an admin a centrally managed way to approve and deny overlay access.

2.2.1 New shell for Airwall Gateways (airsh)

New in this release is **Airwall shell** (airsh), a console that replaces the special login user accounts such as like *mapconfig*, *macinfo*, and *factory reset*. The [Airwall shell](#) provides tab-completion, inline help, and greatly expands your ability to deploy & configure an Airwall Edge Service directly without going into diagnostic mode.

2.2.1 Overlay Intrusion Prevention Monitor (snort)

Intrusion Prevention allows you to activate any number of pre-defined rule sets. Traffic on the overlay is inspected and if a rule matches, an event is created and sent to the Conductor. You can define event actions based on Snort events.

2.2.1 Airwall Gateway Latency improvements

On certain platforms with a single CPU core, the data plane latency has been reduced from 7ms to approximately 2ms. However, it is important to note that the reduction in latency can vary and depends on concurrency, packet sizes, and various other factors, but in general the latency through an Airwall Edge Service is reduced.

2.2.1 Airwall Relay Performance improvements

In version 2.2, we improved the speed of Airwall Relay traffic using XDP acceleration, allowing traffic to scale even more on your existing hardware.

2.2.1 Full tunnel Windows Airwall Agents and Airwall Servers

In prior releases, an Airwall Agent or Airwall Server needs policies to opt-in to the overlay network, the default being *split tunnel*. In version 2.2, an administrator can check a box on the Airwall Agent or Airwall Server in the Conductor to make the default *full tunnel* and capture all network traffic into the overlay, allowing for a few exceptions that may be in the underlay like DNS, AD, etc. Please note this is Windows only; macOS clients and Linux Airwall Servers will be available in a future release.

2.2.1 Multiple VLAN Tags per interface

We now support trunk ports, allowing you to have two or more VLANs configured on an interface. Each VLAN tag makes a new sub-interface. For example, VLAN tag 25 on eth0 creates a virtual interface named eth0.25. These interfaces can go into various port groups. East-West policies in the Conductor can be built between devices in different VLANs. Please note that you can still create bridges between VLANs as you did in version 2.1.x and earlier.

2.2.1 MAPv1 no longer supported

Conductor version 2.2 and beyond will no longer be able to manage Airwall Edge Services running 2.0 and earlier. Please note that this requires you to upgrade your Airwall Edge Services to version 2.0 or later your Conductor to version 2.2. Review the upgrade section at the beginning of this document for more information about the recommended upgrade process.

2.2.1 Dual-use port mode deprecated

Dual-use mode for interfaces is no longer available. Using multiple port groups and trunk ports, it is now much easier to implement split-tunnel with East-West policies. You can add the DNS, AD, and other servers as protected devices to an Airwall Edge Service and give them a separate overlay port group connected to the underlay network. In Conductor, you can then give your protected devices policy to the DNS, AD, etc., servers.

What's New in 2.1

Version 2.1 of our product includes many new features and enhancements.

2.1.6 Modbus TCP to RTU Gateway

We've enhanced our Serial over IP (SoIP) feature with a Modbus TCP to Modbus RTU gateway. After configuring Modbus via the HIPswitch SoIP settings in Conductor, the HIPswitch will accept Modbus TCP commands from servers, issue the commands to serially-connected Modbus RTU device(s), and return the responses via Modbus TCP back to the server. The HIPswitch accepts pipelined requests from the server(s). This provides optimal efficiency for Modbus traffic in terms of throughput, latency, and number of messages as compared to transparent Serial over IP.

2.1.6 DHCP Relay

HIPswitches can now relay DHCP requests to a central DHCP server as an alternative to your existing DHCP server. This allows additional deployment flexibility where extended DHCP options are needed, or an existing DHCP server integrates with other systems such as Active Directory and DNS.



Note: When moving devices from one HIPswitch to a different one, the central DHCP server may issue the same IP address to the device, which could result in policy or routing conflicts depending on your network.

2.1.6 Wireless Underlay Failsafe

The HIPswitch Link Manager, introduced in version 2.1.0, intelligently monitors the health of the underlay connection, detecting when there are no options for the HIPswitch to connect to Conductor or peer HIPswitches. Link Manager is now enhanced to reboot the HIPswitch which may restore the wireless connection to a healthy state.

Occasionally, changes made in the wireless provider network will drop or hang a cellular or WiFi HIPswitch uplink in such a way that the modem cannot recover. Rebooting the HS will force the modem and cell tower or access point to renegotiate their connection; sometimes this restores a healthy connection. This behavior is on by default for wireless models, and can be disabled and configured per HIPswitch in the Conductor UI. You can configure the amount of time Link Manager waits to reboot the HIPswitch after first detecting underlay failure, and a minimum amount of time to wait between reboot attempts. By default, all wireless models enable this feature with a wait-to-reboot value of 10 minutes, and min-wait-between-reboots value of 30 minutes.



Note: See known issue DEV-9877 for additional information in reference to running a HIPswitch on the Microsoft Azure platform.

2.1.6 APAC Modem Support

The HIPswitch cellular expansion module SFF-MOD-MC7430 (PLF-0118-01) is now available for the HIPswitch 150, which includes the Sierra Wireless MC7430 modem for operation in Hong Kong, Macau, and Japan.



Note: Firmware release 2.1.6 is required to use this expansion module.

2.1.6 HIPswitch 250 Series Revision 2 Support

The HIPswitch 250 Revision 2 is now available and includes the following SKUs:

- HIPswitch 250e (PLF-0062-02)
- HIPswitch 250g (PLF-0066-02)
- HIPswitch 250gd (PLF-0111-02)

Revision 2 provides improved SFP compatibility, modem watchdog support, and improved modem carrier compatibility.

2.1.6 Wired Interface Support for Android

The HIPclient for Android now supports wired ethernet connectivity.

2.1.6 Tag integration with HIP invitations

You can now specify tags for HIP invitations, which apply to HIP services as they activate. This makes it easy to organize newly-activated HIP services and, when combined with smart device groups, automatically give them communications policy in overlay networks.

2.1.6 Longer HIPswitch UIDs

HIPswitches which are licensed with a 2.1.6 or higher firmware may generate a longer serial number portion of the UID (up to 20 characters), compared to the previous 12 characters. HIPswitches licensed from a previous release will not change their UID.

2.1.5 FIPS

Tempered Networks now offers FIPS 140-2, based on the HS-500 and Conductor-500 platforms. With FIPS, private keys are stored on the FIPS-certified HSM (hardware security module). The HSM performs all cryptographic operations. For this added key security, performance may be noticeably slower in terms of data plane throughput and firmware update processing. Redundant HA FIPS is not supported at this time.

2.1.5 Improved time management

NTP sync is now configurable from the Conductor. Various improvements have been made to ensure the Conductor and HIPswitch times remain closely synchronized, eliminating time-drift.



Note: We recommend pointing your HIP-enabled servers and clients to the same NTP Time source to ensure proper synchronization.

2.1.5 HIPswitch 75w Series

We now offer the HIPswitch 75 Series with a built-in WiFi module. Software version 2.1.5 does not currently provide WiFi LED status on the outside of the unit, but the WiFi uplink functions correctly. This will be addressed in a future release.

2.1.5 HIPswitch 150e Series

We now offer the HIPswitch 150e base platform, suitable for ICS and SCADA environments and includes 4x Gig-E and 1x SFP port, 1x micro-USB console port, and can be powered by PoE or external single- or dual-power supply. The HS-150 can sustain 75 Mb/s, and burst up to 100 Mb/s. This new platform supports field-upgradeable expansion modules.

2.1.5 HIPswitch 150 Series cellular module

This release supports a cellular expansion module suitable for North American cell carriers, which accepts 3FF Micro SIM cards. ATT, Verizon, T-Mobile, Rogers, and Telus have been field-tested at the time of this release.

2.1.5 HIPswitch 250 Series single- and dual-modem automated recovery

We added an internal watchdog monitor for cell carrier uplink connections. If a HIPswitch cannot connect to Conductor via any means, then occasionally (approx. once per day) it will perform a full reset, which may re-establish the carrier connection in certain environments. This will only occur when the HS-250 has no means of reaching the Conductor or peer HIPswitches.

2.1.5 HIPrelay bandwidth reporting

It is now possible to view the bandwidth of relayed connections between HIP Services in Conductor! An extra tab will appear in Conductor at HIPservice > Reporting > HIPrelay Stats for each HIPrelay. These statistics provide visibility into your network utilization with full-color, layered bandwidth graphs. They are also useful for troubleshooting underlay network relayed connection issues.

2.1.5 Service-specific CPU and memory reporting

For 2.1.5 and above, your HIP Services will report resource utilization more granularly, and you will be able to see this diagnostic information in **HIPswitch > Reporting > Graphs**.

2.1.5 Headless install for Windows HIPclient and HIPserver

You can now perform non-interactive installations of the Windows 7 HIPclient or HIPserver using Microsoft's System Center Configuration Manager (SCCM). Previous releases required manual acknowledgment by an administrator to complete the installation of an unsigned network tap (TAP) driver on Windows. We have patched the driver and obtained Microsoft certification, so this step is no longer necessary.

2.1.5 Tags public API

All basic tagging capabilities released in software version 2.1.4 are exposed in the public API. This includes the ability to index the tags, set or unset tags on taggable objects, such as devices, device groups, HIP Services, HIPservice groups, networks, and people. You can manage tags, retrieve various objects by tag, manage tag expirations, and perform other tag-based actions on several taggable objects at once. Advanced tag management, such as using tags in smart device group rules, or managing monitor event-actions that manipulate tags, will be added in a future release.

2.1.5 Custom CA alerts & public API

Though technically possible, it was difficult to use a non-Airwall CA at scale with your Conductor and Airwall Edge Services. Prior releases required you to manually copy/paste each CSR and cert from the Conductor GUI. Now you can automate the process using new public API calls. This enables a scriptable, scalable Conductor-centric workflow. Also, an admin alert is created in Conductor when custom CA certs are near expiration.

2.1.4 Airwall Agent for Android

With this release, the Airwall Agent is available for Android. Your Android devices can now natively connect to your Airwall overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different Airwall overlays as needed.

2.1.4 Improved Conductor UI Navigation

Several UI elements have been redone to improve navigation:

- Conductor settings are now accessed from the gear icon in the upper right corner of the UI.
- The logged in user profile, API docs, EULA, and sign-out are accessed from the user account icon in the upper right corner of the UI.
- Item names in many lists throughout the UI now actively link to properties pages and dialogs. This greatly simplifies navigation between related elements.

2.1.4 Tags

Tags provide flexible asset management in the Conductor. Devices, Device Groups, Airwall Gateways, Airwall Groups, Overlay Networks, and People can be tagged directly. The Tag information dialog allows you to **Navigate** directly to any tagged item, perform bulk **Actions** (Enable, Disable, or Untag tagged items), and edit **Properties**. Items can be tagged permanently or until you untag them. You can also set an expiration date, which will untag a component after a configurable period of time. You can create tags from the **Tags** page, access from the tag icon in the upper right corner of the UI.

You can also create tags inline while modifying an item's tag members by entering a new tag name and select colors for easy classification. Tags have been integrated into searching and filtering throughout Conductor.

Tags can be used in matching rules to greatly simplify Smart Device Groups. They can also be added to or removed from taggable items in Event Monitor Actions, which allows monitor results to affect overlay network policies. By using tags with these features, you can optimize your workflows. For example, you can create temporary network policies for specific devices, easily revoke policy directly from devices or HIPswitches without having to navigate to a network, and allow multiple admins to keep track of their assets in a single Conductor.

2.1.4 Relay Probes

An Airwall Gateway with this option selected periodically sends probe packets to all of its relays, and use the closest relay when initiating secure tunnels. This reduces the amount of network traffic used to build new tunnels, and allows auto-connect to be turned off. You can find this option in the **Advanced settings** section of a HIPswitch's settings page.

2.1.4 Conductor Diagnostics

Similar to diagnostics offered for Airwall Gateways, the Conductor now has a set of maintenance and diagnostic functions consolidated under the Diagnostics tab of the Settings page. These include Creation or Restoration of a DB Backup, downloading a Conductor support bundle, and viewing a Conductor diagnostic report. Network diagnostics allow you to generate a packet capture on the Conductor interface, ping, and traceroute.

2.1.3 The Airwall 75 Series

The Airwall 75, released with 2.1.3, is designed for medical devices, point of sale systems, and others like building automation controls. It securely connects and protects those endpoints across all networks with little to no change to existing infrastructure. The 75 plug and play design makes universal connectivity and segmentation simple, fast, and cost-effective.

2.1.3 Airwall Agent for Linux

With this release, the Airwall Agent is now available for Linux. Your Linux devices now can natively connect to your Airwall overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different Airwall overlays as needed.

2.1.3 New platform support for Microsoft Azure and Google Cloud

You can now create, manage, and retire Microsoft Azure and Google Cloud HIP Services directly from the Conductor UI.

2.1.3 Support for offline Conductor licensing

We have added support to allow Conductors without access to the public Internet to complete voucher and provisioning requests with our licensing and provisioning server. You can export a sync package, send it to Tempered Networks Support, and import a file containing your licenses back in to your Conductor from a drop-down on the **Settings > Licensing** tab.

2.1.3 New API token system and improved token management

We have updated the API to make tokens more secure. All API requests now require two headers:

- **X-API-Client-ID** is unique by user and can be found on your user preferences page
- **X-API-Token** is generated from your user preferences page. This token is secret, so if you lose it, you must generate a new one. Whenever you refresh your token, all previous tokens will be expired.

The client ID and a refreshed secret token may also be acquired via the API using basic authorization at /api/v1/token/generate. Please refer to the API documentation for details.



Note: The **X-Person-Email** and **X-Person-Token** headers are deprecated and no longer function.

2.1.3 New network creation wizard

New in this release is the ability to quickly create a hub-and-spoke or full mesh network using a simple, wizard-driven UI.

2.1.2 The HIPswitch 250 Series

The Airwall 250 Series is our newest hardware product and the industry's first identity-based industrial IoT gateway for Industrial Control Systems, OT, SCADA, and critical infrastructure. The Airwall 250 includes highly available uplinks over ethernet and up to two different cellular carriers, all actively monitored using fast failover and the ability to prioritize across both cellular and wired links. It also provides 8 x 1 Gbps and 4 x SFP (fiber or copper) with PoE, eliminating the need for ethernet switches and additional power sources. The HIPswitch 250 can also act as a HIPrelay, a feature introduced in version 2.0 of our software.

2.1.2 Airwall Agent for macOS and iOS

With this release, the Airwall Agent is now available for macOS and iOS. Your devices now can natively connect to your IDN overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different IDN overlays as needed. Additionally, integration with Airwall Relay gives you seamless and secure mobility for your computers running Apple's macOS and your devices running iOS.

2.1.2 Link Manager

Link Manager supports all cellular platforms, including our new Airwall 250 Series, providing uplink redundancy and intelligent monitoring for one wired and two cellular uplinks. Dynamic switching occurs based on which port provides the best performance. Default monitors can be customized with your own destinations.

2.1.2 Integration with AWS

You can now create, manage, and retire AWS Airwall Edge Services directly from the Conductor. After creating a template, you can easily create more HIP Services to function as HIPrelays or protect virtual machines in your VPCs.

2.1.2 HIP Invitations

Airwall Invitations, a new feature in 2.1, allows you to add mobile phones, tablets, and computers running a Airwall Agent or Airwall Server to your Airwall solution by sending the user an email containing an invitation. When the user accepts the invitation, the Conductor automatically takes care of all the steps to provision, license, manage, name, group, and create policy for the new Airwall Agent or Airwall Server without manual steps by the administrator. Airwall Invitations can be sent in bulk to entire organizations, and the Conductor will handle the rest.

2.1.2 Improved alerts and monitoring

In this release we added additional monitors, such as the **HTTP GET** monitor that allows you to parse web responses from devices in an overlay. Monitors have been expanded to support device groups and HIPservice groups. The event history graphs will now display frequently or recently triggered monitors.

2.1.2 Improved performance

We made significant performance improvements across the board for all platforms, with virtual Airwall Gateways and the Airwall 400 roughly doubling in performance.

Definitions of Key Terms

Before you get started, you may want to review our list of key terms and definitions you will find in our documentation relating to Tempered products and services.

Product, Technology and Service terms



Note: These terms are specific to Tempered products, technologies, or services and may have additional definitions or descriptions unique to Tempered.

HIP

Host Identity Protocol. The secure protocol that ties our products together.

IF-MAP/MAP/MAP2

Interface to Metadata Access Points. Airwall Edge Services use this client/server protocol to communicate with the Conductor, which provides authentication keys and communication policy to them.

Conductor

The physical, virtual, or cloud-based appliance that centrally manages all connected Airwall Edge Services and devices.

Airwall Edge Service

Any HIP-enabled hardware or software connected to the Conductor. A collective term for all Airwall Gateways, Airwall Agents, and Airwall Servers. Formerly known as HIPservices.

Airwall Gateway

A physical, virtual, or cloud-based appliance that provides overlay network connectivity to connected devices. Formerly known as HIPswitch.

Airwall Agent

A HIP software-based appliance specialized for devices running Windows, macOS, iOS, or Android. Formerly known as HIPclient.

Airwall Server	A HIP software-based appliance specialized for servers running Windows or Linux. Formerly known as HIPserver.
Underlay	This is your existing Layer 2 networks, including the Internet if your Airwall Edge Services traverse it. Your Airwall Gateways and Conductor communicate with each other via this network. Formerly known as Underlay.
Overlay	This is the virtual network, where your protected devices sit behind their respective Airwall Edge Services. Formerly known as Overlay.

Terms related to our technology

 **Note:** These terms are not specific to Tempered products, technologies, or services and have definitions or descriptions relating to networks and networking in general.

Microsegmentation	Compartmentalizing your network into isolated segments in which devices are only exposed to each other when they have a need to communicate.
Multihoming	Connecting a single device to multiple networks, physical and/or virtual.
Tunneling	Encapsulating network traffic in an encrypted connection between two points (e.g. a virtual private network).
Bump-in-the-Wire (BITW)	An antiquated term for a communications device introduced to a legacy system to enhance it. While we rarely use this terminology, it accurately describes our Airwall Gateway line of products, especially when used with legacy systems to enhance security.
Back-haul Interface (BHI)	An interface that carries traffic from a central network to the network's edge. Airwall Edge Services are considered a type of Back-haul Interface, carrying overlay traffic to and from protected devices.
IPsec	A secure network protocol stack for encrypting packets of data sent over an IPv4 network.
Encapsulating Security Payload (ESP)	An encryption protocol used by IPsec.

Legacy and deprecated terms

 **Note:** Although no longer used, older white papers, web articles, and videos may use these terms. Internally, the product may refer to components using these terms as well, such as in log files, for example.

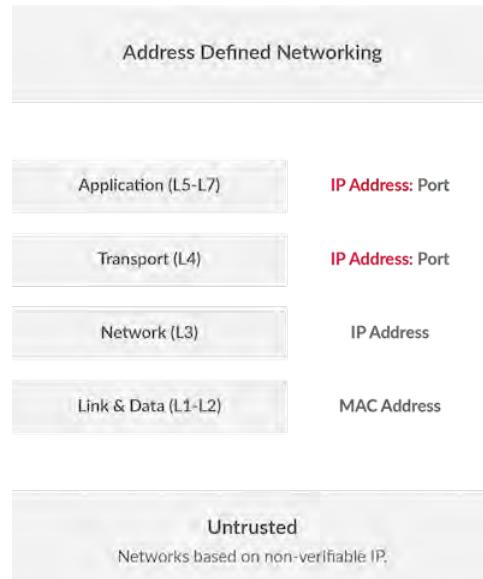
Tempered Networks or Asguard/Asguard Networks	Our previous company names. Sometimes you will see tn , for Tempered Networks, or ama , which stands for Asguard Management Appliance , a previous internal name for the Conductor.
SimpleConnect	Previous term for the Conductor. Sometimes you will see sc as a prefix in log entries and exported files, meaning that they are related to the Conductor.
Endbox	Previous term for an Airwall Edge Service. This term is still used internally, so you might see it in logs.

Host Identity Protocol (HIP)

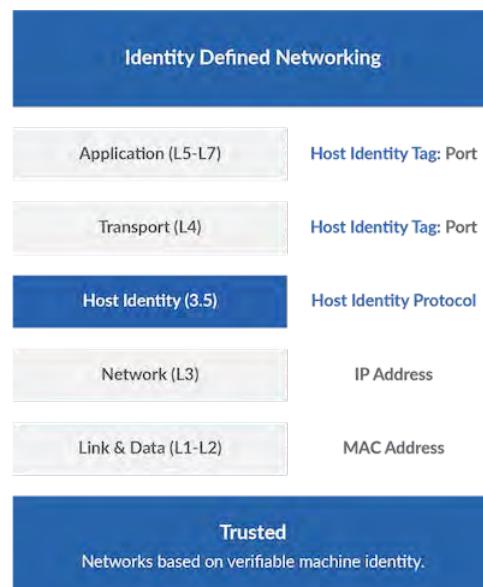
HIP is an open standard that delivers a better approach to security, authentication, mobility, and resiliency for networks. The protocol has been under development for over 20 years in coordination with several Fortune 500 companies and standards bodies, before being officially approved in 2015 by the IETF. Tempered is the first company to commercially leverage the technology.

HIP separates the role of an IP address as both host identity and location within a network, such that hosts are instead identified using cryptographic identities in the form of public keys. We can then define device-to-device trust relationships based on the host identity instead of the IP address.

In a traditional networking model, referred to below as address-defined networking, routing is done via IP addresses. The upper layers of the standard networking framework, or stack, represent software that implements network services like encryption and connection management. The lower layers of the framework implement hardware-related functions like routing, addressing, and flow control.



In an identity-defined networking model, the HIP identity layer inserts itself in the stack between the network and transport layers. As a result, applications and transport protocols use a host identity tag instead of an IP address. Each host is now identified on the network with a unique cryptographic identity, while the IP address is used only for location.



The Airwall Solution

The Airwall Solution makes your connected ‘things’ invisible. It eliminates network-based attacks, secures remote access at scale, and extends the life of existing infrastructure investments. It effectively reduces cyber risk and makes securing a corporate network less complex.

Airwall addresses the problems inherent in the existing solutions that tell you you need more firewalls, VPNs, VLANs, ACLs, SSH keys, etc., but that you’re never really secure.

The problems with TCP/IP

The root of the problems with the existing solutions lies within IP’s own shortcomings. TCP/IP was created with connectivity, not security, in mind. As the number of devices on a network increases, so too does the vulnerability to cyber attacks and the complexity of IP-based network security. The answer to these challenges is a trusted networking architecture model based on cryptographic identities.

Airwall offers a better way

The Airwall Solution is an infinitely better way to keep it all safe. It enables you to:

- Secure first, and connect later.
- Provide secure access and total invisibility at any scale, across any network.
- Secure your local datacenter and your global infrastructure with a solution that allows connections across both.
- Secure every endpoint in your network, with true micro-segmentation and secure remote access.

Make all of your things Invisible

Airwall allows only trusted and cryptographically-identified “things” to connect, creating a network that is more secure and flexible than the traditional TCP/IP model. The network just doesn’t respond to any non-trusted sources, so all of your “things” are protected.

Easily deployed

The Airwall Solution enables you to easily deploy and extend a unified, trust-based, and encrypted network. Micro, macro, and cross-region segmentation, as well as global IP mobility are simple to set up. Deploying and maintaining intra-cloud (region to region), cloud-to-cloud, and cloud-to-data center cryptographic trust-based communications becomes simple, verifiable, and secure.

Airwall works on Existing Networks

Airwall requires little to no modification of the underlying network or security infrastructure. It provides a simple, policy-based configuration of devices or groups of devices that are explicitly trusted based on allowlisting. This trust, based on unique cryptographic identities, determines what systems or machines can initiate and establish communication before any data is exchanged.

The Airwall Solution is set up using the **Airwall Conductor**, an intuitive, visual, point-and-click management and orchestration engine. The Conductor easily manages a network, regardless of how many devices are part of it. Our Airwall Edge Services are software products delivered in different forms to support our commitment to securing any device, anywhere.

Built on the Host Identity Protocol (HIP)

The Tempered Airwall Solution is the first to use **Host Identity Protocol (HIP)**, an open-standard network security protocol that provides provable host identities. This technology has been recognized by the **Internet Engineering Task Force (IETF)** as the next possible major improvement in IP architecture, making HIP a true paradigm shift in networking that solves the fundamental security flaws of TCP/IP. HIP was formally ratified by the IETF in 2015, capping 15 years of successful development and deployment in coordination with several major companies (Boeing, Verizon, Nokia) and standards bodies (Trusted Computing Group, IEEE 802).

Instead of using the flawed dual function of the IP address, HIP assigns identity with 2048-bit RSA public keys and assigns location with the original IP address. These identities are permanent, location-independent cryptographic

identities that are connected to machines or networks, enabling security by default with verifiable authentication, authorization, and host-to-host encryption.

Within TCP/IP, there are two globally-deployed namespaces that allow the Airwall Solution to uniquely identify a host or service: IP addresses and DNS names. However, due to the fundamental flaws of TCP/IP, both namespaces are problematic for networks. HIP introduces a third option for namespaces: the **Host Identity Namespace (HIN)**. The HIN is compatible with the current namespaces, and provides global IP mobility and security policies based on unique cryptographic identities. It overcomes many of the fragile and costly challenges of traditional TCP/IP networking.

How to get support

You can often find answers to your questions in Airwall helpthe guide, or by logging in to your **Support** account and searching the knowledge base articles. If you still cannot find what you are looking for, you can contact support for help.



Note: You must have a current support contract with Tempered to open a support ticket.

There are several ways to contact support.

Open a case on the Tempered Support Web Portal

1. Go to <https://www.tempered.io/support/supportReq.html>.
2. Sign in using your support account log in.
3. Click + or **New**.
4. Fill in the name and contact information.
5. Provide the **Information to Include** listed below.
6. Attach the support bundle from the affected devices.
7. For network issues, attach a packet capture.

Contact Tempered Support via email

1. Send an email message to support@tempered.io.
2. Provide the **Information to Include** listed below.
3. Attach your support bundle to the email.
4. For network issues, attach a packet capture.

Information to Include

Provide the following information when you open a case with Tempered Support:

- A full description of the issue, including the following details:
 - The symptoms of the issue, including a brief description of all systems applicable to the configuration.
 - The approximate time the issue first occurred.
 - The number of times the issue has recurred.
 - Any error output provided by the system.
 - Steps to reproduce the issue.
 - Any changes you made to the system close to when the issue first occurred.
 - Any steps you've taken to resolve the issue.
 - Whether this is a new implementation.
 - How many data centers and devices are applicable to the configuration.
 - Which devices are affected by the issue.
- A description of the impact the issue is having on your site.
- Days and times you are available to work on the issue, and any alternative contacts that can work on the issue if you are not available.

Get a Support Bundle

The Support Bundle is the technical information about the device. To best answer support issues, Tempered Support needs the Support Bundle from the Conductor and Support Bundles from any Airwall Gateway, Airwall Agent, and/or Airwall Server that is part of the issue you are reporting. For more assistance, see [Create a support bundle from the Conductor](#) on page 412.

Get a Packet capture

If the issue involves the network, perform a packet capture while the issue is occurring. Provide this packet capture when you open the case. For more assistance, see [Troubleshoot an Airwall Gateway by using packet capture](#) on page 415.

Copyrights



Note: The Airwall Agent and Airwall Server for Microsoft Windows deploy an open source TAP driver as part of their installation. In compliance with GPL distribution requirements, the source code is available here: <https://temperedsoftware.s3.amazonaws.com/clients/windows/drivers/tap-windows6-master.zip>

All rights reserved by Tempered, Inc. ("Tempered") and its licensors.

Copyright © 2012- 2021

This source code and the methodology disclosed by it include proprietary and confidential information belonging to Tempered and its licensors ("Source Code"). The Source Code may not be copied, modified, or distributed without the prior express written permission of Tempered.

By using the Source Code, You agree to be bound by these terms and conditions of use. You acknowledge that this is only a limited, nonexclusive, non-transferable license. Tempered and its licensors remain the owners of all titles, rights, and interests in the Source Code. Further, use of the Source Code is governed by the terms and conditions of Your license agreement with Tempered regarding the Source Code, which license agreement is incorporated herein by reference.

Use of the Source Code is permitted to You only as a Partner of Tempered under written agreement and for no other purpose than the partnered work You are doing with Tempered. The Source Code may not be disclosed to or used by anyone other than Your employees or contractors working on Tempered product development projects. You may not disclose, assign, sublicense, lease, or in any other way transfer the Source Code to any third party without the prior express written consent of Tempered. Any product developed using the Source Code may be distributed, displayed, licensed, sold, or used in object code format only and as specified in a written license with Tempered permitting such distribution, display, license, sale or use.

Tempered has the right to terminate this License Agreement and Your right to use the Source Code upon any material breach of the License Agreement by You.

You agree to defend and indemnify Tempered and to hold Tempered harmless from all claims, losses,damages, complaints, or expenses connected with or resulting from Your business operations relating to use of the Source Code.

THE SOURCE CODE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOURCE CODE OR THE USE OR OTHER DEALINGS IN THE SOURCE CODE.

Host Identity Protocol

Copyright © 2012-2021 Tempered, Inc. All Rights Reserved.

Tempered, Inc. ("Tempered"), hereby grants worldwide permission, free of charge and without a signed licensing agreement, for the duration of the copyright, to any person obtaining a copy of this software and associated documentation files ("The Software"), the right to deal in The Software without restriction, including, without limitation, the right to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of The Software, to

make, publish, distribute, and/or sell derivative works based on The Software, and to permit persons to whom The Software is furnished to do so, subject to the following conditions:

The above copyright notice and this Permission Notice shall be included in all copies or substantial portions of The Software and in all modifications and distributions of The Software, including derivative works based on The Software. Neither the names of Tempered nor the Authors, nor any of their trademarks or service marks, may be used to endorse products derived from The Software without the express prior permission of Tempered.

Except as expressly stated herein, nothing in this Permission Notice grants any license to Tempered's trademarks, service marks, copyrights, patents, trade secrets, or other intellectual property. No license is granted to the trademarks of Tempered even if such marks are included in The Software. Nothing in this Permission Notice shall be interpreted to prohibit Tempered from licensing under terms different from this Permission Notice any Original Work that Tempered otherwise would have a right to license.

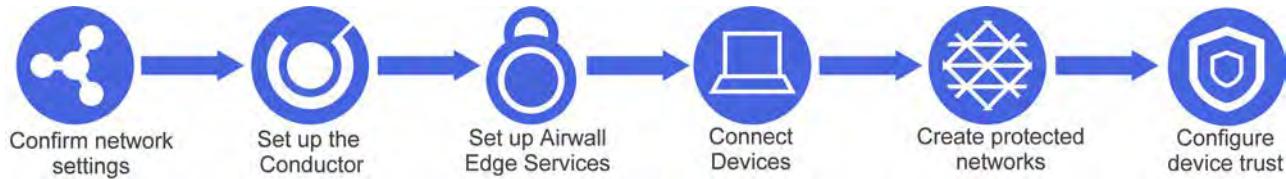
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. THE AUTHORS AND COPYRIGHT HOLDERS HAVE NO OBLIGATION UNDER THIS PERMISSION NOTICE TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS TO THE SOFTWARE.

Deploy an Airwall secure network

Deploy, Install, Configure, License

Building an Airwall Solution requires a minimum of three components: An Airwall Conductor and two or more Airwall Edge Services with devices attached behind them. You can manage these Airwall Edge Services and their attached devices from the Conductor dashboard. The Airwall Edge Services create a zero-trust virtual protected network. The Conductor acts as a centralized management dashboard for the network, pushing policy and trust information to the Airwall Edge Services. Every Airwall Edge Service within the protected network knows the network layer and state of its peers, and every peer maintains Identity-Based Routing (IDR) tables.

A typical deployment requires the following steps:



Note: If you are installing a physical Conductor or Airwall Edge Service, make sure you are familiar with your model, including the variety of power options and physical installation steps before you begin your deployment. Refer to the Platform or Install Guide included with your hardware.



Tip: For additional information about the Airwall Solution, see the [What makes up an Airwall secure network?](#) on page 119 in the [Get Started with the Airwall Solution](#) on page 117 section.



Tip: For additional information about the Airwall Solution, see [What makes up an Airwall Secure Network](#) in the [Get Started](#) section of our online documentation.

Deployment Checklist

A checklist for deploying the Airwall Solution

Also check out:

- The Airshell command setup-ui at [Airwall Gateway Airshell console commands – airsh](#) on page 305.
- Startup tutorials for the Conductor at [Get Started using Conductor Help and Tutorials](#) on page 118.

A typical deployment requires the following steps:

1. Plan your deployment.
2. [Confirm your Network Settings](#) on page 156.
3. [Deploy and Configure a Conductor](#) on page 165.
4. [Deploy and Configure Airwall Edge Services](#) on page 236
 - a) [Set up Airwall Gateways](#) on page 237
 - b) [Connect People's Devices to your Airwall secure network](#) on page 54
 - c) [Configure Airwall Edge Service Settings](#) on page 304
 - d) [License a Conductor and Airwall Edge Services](#) on page 159
5. [Connect and Configure Devices](#) on page 351.
6. [Create and Manage an Overlay \(Protected\) Network](#) on page 355.
7. [Configure Device Trust](#) on page 360

If you have special configuration needs, see [Configure Advanced Airwall Edge Service Options](#) on page 319 for different options on how to configure Airwall Edge Services.

Confirm your Network Settings

Check that your network is set up to start deploying the Airwall Solution.

Your existing network is the underlay network, made up of your existing private networks and the Internet. It's any network that you connect an Airwall Edge Service to, and any network used to communicate between other Airwall Edge Services in your Airwall deployment. For Airwall to work correctly, all components must be able to communicate with each other from where they are installed.

The Conductor

The Conductor is the central management dashboard for all Airwall Edge Services. It tells the Airwall Edge Services how to contact one another and enforces policies on the protected network – allowing or preventing communication between devices. It also manages licensing and provides diagnostic tools.

Your Conductor can be either virtual or physical and can be configured in a high-availability (HA) pair. It passes no protected network traffic and does not communicate with the HIP protocol.

The Conductor must have at least two network interfaces. The recommended configuration is as follows:

Port 1	Connect to the Internet, either directly or with port forwarding.
Port 2	Connect to your Local Area Network (underlay)

For the Conductor to work, it must be able to listen on the following ports:

TCP 8096 (MAP)	This is the port in which Airwall Edge Services communicate with the Conductor.
TCP 443 (HTTPS)	This is the port in which the Conductor Management can be accessed.

Airwall Edge Services

An Airwall Edge Service carries out or facilitates the connectivity between two connecting devices.

A Airwall Gateway is a network appliance that allows Ethernet devices to be added to the protected network (Overlay). It connects to a Conductor via a Metadata Access Point (MAP) for policy and peer addresses, and it connects to peer Airwall Edge Services to establish secure tunnels between locations.

An Airwall Gateway can be either virtual or physical and can be configured in an HA pair. It passes traffic between devices over a HIP tunnel.

An Airwall Gateway must have at least two network interfaces. The recommended configuration is as follows:

Port 1

Connect to the Local Area Network (Underlay). Must be able to reach the Conductor and other Airwall Edge Services.

Port 2

Protected Device Network (Overlay). Must be able to reach the devices to add to the overlay.

It is possible to connect Ports 1 & 2 to the same network and provide existing device access to the Overlay, without isolating the protected devices inside of a separate network segment.

For the Airwall Gateway to work, it must have *outbound* connectivity on the following ports:

TCP 8096 (MAP)

Must have outbound connectivity to MAP to the Conductor.

UDP 10500 (HIP)

Must have outbound connectivity to HIP and to any other Airwall Edge Service is a must to communicate with.

At least one Airwall Gateway on one end of a tunnel must also be able to listen on the following port:

UDP 10500 (HIP)

Must have outbound connectivity to HIP and to any other Airwall Edge Service is must communicate with.

Alternately, if Airwall Edge Services cannot be configured to listen for incoming connections, you can employ an Airwall Relay to get around a network address translation (NAT).

Airwall Relays

An Airwall Relay is, typically, a virtual cloud-hosted appliance, running the Airwall Gateway 300v VM. It is able to listen for HIP traffic, allowing Airwall Gateways behind firewalls and routers to establish a tunnel between each other even when NATed.

For the Airwall Relay to work, it must have outbound connectivity on the following ports:

TCP 8096 (MAP)

Must have outbound connectivity to MAP to the Conductor.

UDP 10500 (HIP)

Must have outbound connectivity to HIP and to any other Airwall Edge Service is must communicate with.

It must also be able to listen on the following port:

UDP 10500 (HIP)

This is the port, in which Airwall Edge Services communicate with the Conductor.

Airwall Relays are still considered a type of Airwall Edge Service, but they serve a special role. Any Airwall Gateway - physical or virtual - can be turned into an Airwall Relay. Once configured as an Airwall Relay, it is not advisable to add any devices to it, but instead use it exclusively to bridge Airwall Edge Services that are not able to listen for incoming connections.

Changing network ports

You can change the MAP and HIP ports from their defaults of 8096 and 10500 in the Conductor. This will change the settings for all Airwall Gateways connected to that Conductor.

These settings rarely need to be adjusted. When they are, it is either to get around some immutable firewall settings or to add extra security by using atypical ports.



Note: If you change the MAP port, you will need to manually reconfigure all Airwall Edge Services to point to the Conductor with the new port. This might involve traveling to remote sites and putting devices into diagnostic mode, so adjust this setting carefully.

If you change the Airwall Edge Service port, the change takes effect on all Airwall Edge Services connected to the Conductor, so make certain that they have the proper outbound connectivity and port forwarding configured before adjusting this setting.

To change the default ports:

1. In the Conductor, go to **Settings**.
2. Find the **Advanced** section near the bottom of the **Settings** page. Next to **Global HIPservice settings**, click **Edit Settings**.
3. Under **Port settings**, change the default ports, and click **Save**.

HIP and MAP Diagrams

Below are some diagrams illustrating successful and unsuccessful MAP and HIP configurations:

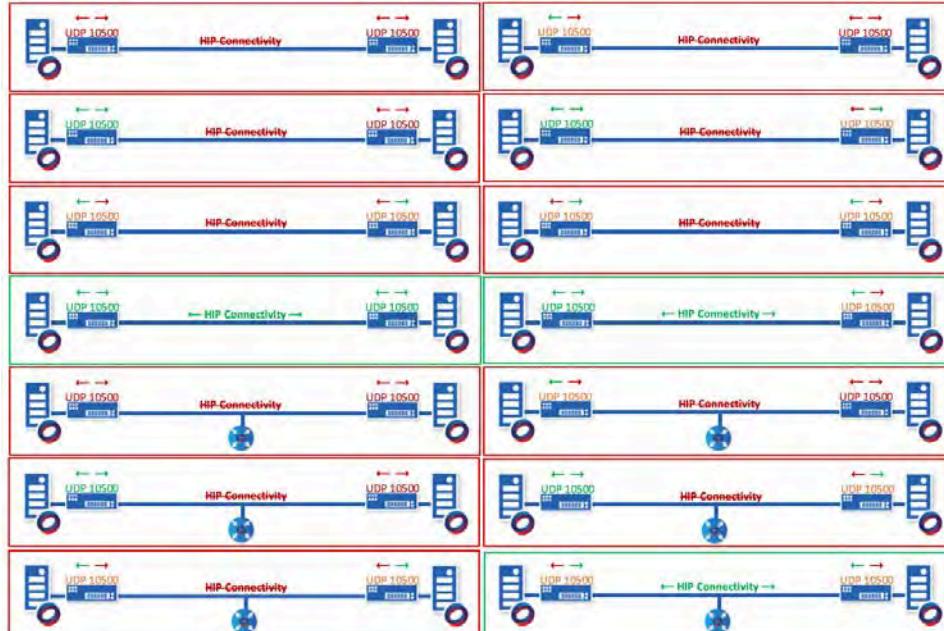


Figure 3: HIP configurations

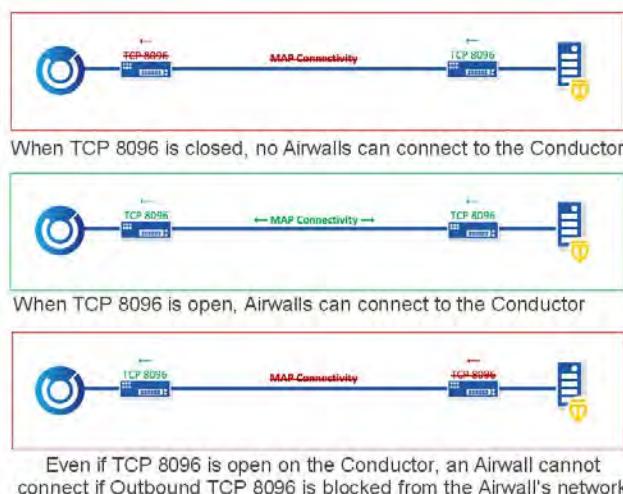


Figure 4: MAP configurations

Check Your Underlay Settings

Check the following settings to confirm they're set for the new ports:

Firewalls

If a firewall is enabled between the Conductor and Airwall Edge Services in the solution, you must open the required firewall ports.

DHCP and DNS

If you prefer to configure your Conductor with a hostname or assign Airwall Edge Services IP addresses using DHCP, confirm that the underlay's DHCP and DNS settings are configured to support it.

Private Network Conductor

If the Conductor is located in a private network, either a firewall or router must provide a static public IP address so the Conductor can be reached by Airwall Edge Services outside the private network.

Private Network Airwall Gateway

If Airwall Edge Services located in a private network need to be accessed by Airwall Gateways outside the private network, a firewall or router must provide a static public IP address so the Airwall Edge Services can communicate.

License a Conductor and Airwall Edge Services

Everything you need to know about licensing your Conductor and Airwall Edge Services.

How Airwall Licensing Works

How licensing works in your Airwall Solution.

Tempered requires a license for each Conductor and Airwall Edge Service you have in use. Certain configurations also require add-on licenses, such as configuring an Airwall Gateway as an Airwall Relay.

When you purchase licenses, you receive a voucher code that allows you to apply your purchased licenses to a Conductor, or to Airwall Edge Services in a Conductor. The Conductor automatically consolidates licensing vouchers.

There is a significant difference between Conductor licenses and Airwall Edge Services licenses -- Conductor licenses are not transferrable, while Airwall Edge Service licenses are. More specifically:

- Conductor licenses **cannot** be reused or transferred once you've used it to license a Conductor.
- Airwall Edge Services licenses **can** be reused and are transferrable by type, and across Conductors. Some examples:
 - In a Conductor, you can delete a license from one Airwall Gateway-150 by revoking it and reassign the license to a different Airwall Gateway-150.
 - You **cannot** transfer a license from one type of Airwall Edge Service to another type.

You must have enough licenses available in your Conductor before you can provision Airwall Edge Services. For a list of the Airwall Edge Service licenses you have available, see the **Licensing** tab under Conductor **Settings**.

To purchase new or renew expired licenses, contact sales@tempered.io.

For how-to instructions on licensing and transferring licensing, see these topics:

- **License your Conductor**, see the **License and Provisioning** section in [Deploy a Physical Conductor](#). Licensing and provisioning is the same for physical and virtual Conductors.
- License Airwall Edge Services, see [Provision and License Airwall Edge Services](#) on page 161.
- View your Licenses in Conductor, see [View Licenses in Conductor](#) on page 161.
- Transfer a License to Another Airwall Edge Service, see [Transfer an Airwall Edge Service License to Another Airwall Edge Service](#) on page 164.

- License an Isolated Conductor and Airwall Edge Services, see [License a Conductor and Airwall Edge Services in an Isolated Environment](#) on page 164.

License and Provision a Conductor (v2.2.8 and earlier)

To get a Conductor up and running, you need license and provision it. You need your licensing voucher to complete these steps.

Supported Versions

Conductor v2.2.8 and earlier



Note: For v2.2.10 and later, licensing and provisioning is included in the Initial Conductor configuration wizard. Start at [Log in and Configure the Conductor](#) on page 169.

In v2.2.8 and earlier, you license the Conductor, and then [Log in and Configure the Conductor](#) on page 169.

1. If you have a physical Conductor, apply power to it, and connect a computer to Port 1 on the Conductor hardware using an Ethernet cable. Refer to your unit's Platform Guide for specific instructions.
2. In a web browser:
 - **Physical Conductor** – go to: <https://192.168.56.2>
 - **Cloud Conductor** – Click the link in your order email, or go to the public IP you set up when creating your Conductor.

The Conductor **Provisioning** page opens so you can license your Conductor.

3. If you have a proxy server between your Conductor and the Tempered licensing server, under **Disable network proxy settings**, configure proxy server settings to allow your Conductor to reach the licensing server.
4. If you are licensing an isolated (dark) Conductor, you will use the **Disable secure offline sync** section. For more details, see [License a Conductor and Airwall Edge Services in an Isolated Environment](#) on page 164.
5. In the **Voucher code** box, enter the voucher code you received from Tempered.
6. Click **Provision now**. It takes a moment to finish applying the voucher. Once complete, you should see the following:

7. Select [Click here to start using the Conductor](#).
8. [Log in and Configure the Conductor](#) on page 169.

Add Airwall Edge Service Licenses to the Conductor

The first step in licensing Airwall Edge Services is to add your licensing vouchers to the Conductor.

To add Airwall Edge Service licenses:

1. In Conductor, open **Settings**, and go to the **Licensing** tab.
2. Click **Enter Voucher**.
3. Type or paste your Voucher code, and click **Enter**. The licenses are added to your pool of licenses on the **Licensing** page.



Note: The Conductor automatically consolidates licensing vouchers.

View Licenses in Conductor

See what licenses you have available in the Conductor.



Note: Only Airwall Edge Service licenses are shown in the Conductor. Your Conductor license is not shown.



Note: The Conductor automatically consolidates licensing vouchers.

1. In Conductor, open **Settings**, and go to the **Licensing** tab.
2. Under **Licenses**, you can see the Airwall Edge Services licenses you have, and how many are in use.
3. Select a specific Airwall Edge Service license if you want to view your license count, type, and expiration date.

Provision and License Airwall Edge Services

How to provision and license Airwall Edge Services. You need to [Add Airwall Edge Service Licenses to the Conductor](#) on page 160 before you can provision and license Airwall Edge Services.

1. In Conductor, open **Settings**, and go to the **Licensing** page.
2. If you have a license voucher, [Add Airwall Edge Service Licenses to the Conductor](#) on page 160. If you don't have a license voucher, contact sales@tempered.io to get one before continuing.
3. Install the Airwall Edge Services you want to license and connect them to the Conductor. For more information, see [Deploy and Configure Airwall Edge Services](#) on page 236 and [Connect Airwall Gateways to the Conductor](#) on page 245.
4. Under **Provisioning Requests**, select the check boxes for the Airwall Edge Services you want to provision, and under the **Actions** dropdown, click **Grant Request** to provision your Airwall Edge Services. They should reconnect to the Conductor and appear in your Airwall Edge Services list as unmanaged.



Note: You can also grant provisioning requests from the **Provisioning** tab on the Dashboard.

5. On pre 2.2x Conductors, click **Sync**.
6. On the Conductor dashboard, click the **Show all Airwalls** box and filter the Airwall Edge Services by unmanaged.
7. In the row for the Airwall Edge Service you want to license, in the far right column, click the arrow to open the drop down menu, and select **Manage Airwalls**.

Airwall™ edge services		
Airwall	Model	Status
AW-500 Physical BHI@40130#E17C6E5801100057	Airwall-500 v2.2.3	10.10.24.21 [status icons]
Cloud Airwall Relay BHI@40130#EC2397DB7AAE	Airwall-300v v2.2.3	172.16.0.60 [status icons]

Provision Airwall Gateways using Activation Codes

If you are deploying Airwall Gateways, you can use Activation codes to quickly set up and provision them using the console and `airsh`.

When you deploy Airwall Gateways using activation codes, they are automatically managed in the Conductor as they connect, and put into any **Airwall groups** you specified when creating the activation codes.

Note: Console access is required to input the activation code on Airwall Gateways. Some cloud providers do not provide console access to their servers (notably AWS), so you will need to provision them in a different way.

Before you begin

- Make sure the Airwall Gateways you are using can be accessed using the console. If you do not have console access, you need to deploy them in a different way. See [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160.
- Set up **Airwall groups** for the deployed Airwall Gateways.
- Set up any tags you'd like to use for the deployed Airwall Gateways.
- Determine how many Airwall Gateways you want to deploy, and how many are in each group. Go through this procedure for each group of Airwall Gateways.

To deploy Airwall Gateways using activation codes, you need to:

1. Create the activation codes
2. Use the console to apply the activation codes to the Airwall Gateways.
3. License the Airwall Gateways as described in [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160.

Create Activation Codes

1. In Conductor, go to **Airwalls**, and open **Airwall Invitations**.
2. Click **Create Airwall Invitations**.
3. On the **Airwall Invitations** page, select **Download activation codes and distribute them manually**, and enter how many Airwall Gateways are in this group. Click **Next**.
4. Select how the Airwall Gateways are named as they connect to the Conductor. Click in the **Generated Airwall name** box for help with how to dynamically create names.

The screenshot shows the 'Airwall Invitations' configuration dialog. At the top, it says 'Configure settings for how to download, install and activate Airwalls'. Below that, there are two main sections: 'Generated Airwall name' and 'Activation code expiration date'. The 'Generated Airwall name' section contains a text input field with the value `\${airwall_type}` highlighted. To the right of this field is a descriptive note: 'Dynamically name Airwall agents when they connect to the Conductor by enclosing them in \${field_name}'. The 'Activation code expiration date' section contains a text input field with the value '06/26/2020'. To the right of this field is a list of 'Available fields': 'email - User's email', 'email_name - User's email without domain', 'airwall_type - Installed Airwall type', and 'ip - Airwall agent's overlay device IP'. At the bottom of the dialog are three buttons: '<< Back', '>> Next', and 'Cancel'.

5. Change the **Activation code expiration date**, if needed, and select **Next**.

- On the **Additional settings** page, select the Airwall groups and tags you want to apply to this group of Airwall Gateways.

Note: You can skip the other options, as they are for Airwall Agents and Servers only.

Airwall Invitations

Additional settings used when activating Airwall agents via invitation.

Overlay device IP network (CIDR) *
e.g. 192.168.16.0/20

Overlay networks *
Add an entry

Device groups *
Add an entry

Airwall groups
Group 1

Tags ?
building2, waponi

* Only applies to Airwall agents when using an activation code

<< Back Generate Cancel

- Click **Generate**.
- Copy or download the activation codes. If you download the codes, the text file includes a summary of the options you've chosen for this group of activation codes.

Configuration	
Profile name:	Conductor hostname or IP: cond.example.com
Generated Airwall name:	<code> \${airwall_type}-\${ip}-group1</code>
Activation code expiration date:	06/19/2020
Overlay device IP network (CIDR):	undefined
Overlay networks:	
Device groups:	
Airwall groups:	Group 1
Tags:	building2, waponi
Activation codes	
<pre>702d2fce3wee 8z130f85eed9 99508e9090qc</pre>	

You're now ready to provision Airwall Gateways using these activation codes.

Deploy Airwall Gateways using Activation Codes

- Plug in the Airwall Gateways you want to provision, and connect them to a network where they can reach the Conductor.

2. For physical Airwall Gateways, connect your laptop using the console port. For details, see [Connecting to the console port on an Airwall Gateway](#) on page 250. For console access on your cloud and virtual gateways, consult your cloud or virtual provider.
3. At the console, log in with name: `airsh`, and password: `airsh`
4. Use the `airsh activate` command, and enter your activation code when prompted.
5. To finish setting up the Airwall Gateway, use `airsh` to also add the Conductor URL and map port (if not using the standard port). See [Airwall Gateway Airshell console commands – airsh](#) on page 305.
6. Repeat with any other Airwall Gateways you want to provision, using a different activation code for each one.

Once you've set the activation code and Conductor URL, the Airwall Gateways will automatically connect to the Conductor, and be provisioned and managed in the Conductor using the options you selected when creating the activation codes.

You can now license your Airwall Gateways. See the License section of [Provision and License Airwall Edge Services](#) on page 161.

Transfer an Airwall Edge Service License to Another Airwall Edge Service

You can transfer Airwall Edge Service licenses within the Conductor.

There are two ways to transfer a license from one Airwall Edge Service to another:

- **Replace** – Replacing an Airwall Edge Service transfers all of the settings from the replaced Airwall Edge Service along with the license. Follow the instructions in [Replace an Airwall Gateway](#) on page 111.
- **Revoke** – Revoking an Airwall Edge Service frees only the license for use, and does not transfer the settings.

Transfer a license by Revoking the Airwall Edge Service

1. Make sure the Airwall Edge Service you want to transfer the license to is installed and provisioned, but unmanaged (unlicensed).
2. Revoke the Airwall Edge Service you want to un-license. For details, see [Revoke and Reactivate an Airwall Edge Service](#) on page 419.
3. On the Conductor dashboard, filter the Airwall Edge Services by unmanaged.
4. Click the drop down on the Airwall Edge Service you want to license, and click **Manage Airwalls**.

Renew Expired Licenses

To renew Airwall Edge Service licenses:

1. Contact sales@tempered.io to renew your subscriptions.
2. Once you've received confirmation from Tempered that your subscription has been renewed, in Conductor, open **Settings**, and go to the **Licensing** tab.
3. On the right top, click **Full Sync** to update your vouchers.



Note: If Tempered provides new vouchers, see [Add Airwall Edge Service Licenses to the Conductor](#) on page 160.

License a Conductor and Airwall Edge Services in an Isolated Environment

To license a Conductor and Airwall Edge Services in an Isolated environment (also commonly called a dark or offline environment), you need to take a few additional steps.

To license an Isolated Conductor

1. On the Tempered Conductor Provisioning page, where it's asking for a voucher code, enter the voucher you received when you purchased the Conductor.
2. Click **Enable secure offline sync**.
3. Click **Export encrypted package**.
4. Save the exported package on the Conductor, and copy the package to a USB drive or other removable device.
5. Mail the package to support@tempered.io for licensing.
6. When Customer Success sends you your encrypted licensing package, download it to a USB drive.

7. Click **Import encrypted package** (you may need to click **Enable secure offline sync** again to show the page), select the package you downloaded, and click **Import**.
8. After the package is opened and finished processing, your Conductor is licensed, and will move to the **Log In** page.

Follow the steps from starting at **Log In and Configure** in [Deploy a Physical Conductor](#).

To provision and license Isolated Airwall Edge Services

1. In the licensed Isolated Conductor, open **Settings**, and go to the **Licensing** page.
2. If you have a license voucher, [Add Airwall Edge Service Licenses to the Conductor](#) on page 160. If you don't have a license voucher, contact sales@tempered.io to get one before continuing.
3. Under **Secure offline Conductor**, select **Enabled** to enable offline licensing.
4. Install the Airwall Edge Services you want to license and connect them to the Conductor. For more information, see [Connect Airwall Gateways to the Conductor](#) on page 245.
5. Under **Provisioning Requests**, select the check boxes for the Airwall Edge Services you want to provision, and under the **Actions** dropdown, click **Grant**.
6. Click **Export encrypted package**, and click **Save**.
7. Mail the package to support@tempered.io for licensing.
8. When Customer Success sends you your encrypted licensing package, download it.
9. In the Conductor, on the **Licensing** page, click **Import encrypted package**
10. Select the package you downloaded, and click **Import**.
11. After the package is opened and finished processing, your Airwall Edge Services are provisioned. They should reconnect to the Conductor and appear in your Airwall Edge Services list as unmanaged.
12. Click the drop down on the Airwall Edge Service you want to license, and click **Manage Airwalls**.

Deploy and Configure a Conductor

The Airwall Conductor helps you deploy, configure, administer, and update your Airwall Solution.

Deploy a Conductor

To set up a Conductor for the first time, you need to configure a few basic settings. After completing the following, you can connect the Conductor to your underlay.

Before you begin these steps

The Conductor manages policy for all distributed Airwall Edge Services, delivering simple control of the network. Confirm your existing network settings such as DHCP, DNS and firewalls to decide where your Airwall solution will exist within your environment. For more information, see [Confirm your Network Settings](#) on page 156.



Important: Do not connect any Airwall Edge Services or hardware until after the Conductor is configured.



Note: The Conductor uses a Tempered security certificate. This certificate is anchored to the Tempered Certificate Authority (CA). You may need to explicitly trust the certificate to connect to the user interface. If you would like to use your own certificate, see [Install a Custom CA Certificate Chain](#) on page 201.

Conductor Configuration Wizard Settings

Here are the settings you can configure in the Conductor Configuration Wizard.

For steps, see [Log in and Configure the Conductor](#) on page 169. For more settings see [Best Practices for Conductor Configuration](#) on page 198 and [Configure a Conductor](#) on page 198.

Supported Versions

v2.2.10 and later Conductor

Wizard page	Setting	Description
Define hostname settings	Hostname and Domain name	Enter a hostname and domain name to create a friendly URL for your Conductor. See Configure a Conductor IP, Friendly URL, or Port on page 198.
Configure network adapters	Enable network adapter	<p>Set up the Network adapters to communicate with your existing network (the underlay). By default:</p> <ul style="list-style-type: none"> For physical and virtual Conductors, Network adapter 1 is configured with a static IP address of 192.168.56.2. For cloud Conductors, the IP address should match the Internal IP or public IP of your Conductor instance. Network adapter 2 is configured for DHCP IP addressing.
	Enable web access to Conductor	This setting enables or disables the web server (the Conductor UI) on the port. You have to have at least one enabled, unless they're both DHCP, then they both have to have it enabled.
	Network configuration	
	Static routes	Define static routes for each network interface if required for communication.
Apply network configuration	Apply	Confirm that the network settings are correct, then select Apply . If the network configuration has been changed, then you may need to manually navigate to the new location in your browser.
Create a second administrative account	Fill in the Username and other details for a second administrative account.	It's a best practice to only use the 'admin' account for top-level administration. Creating user accounts for each person who will be administering the Conductor lets you see who is making changes in the system when you review log details.

Wizard page	Setting	Description
Configure date and time settings	Use NTP and NTP Servers	Enable Use NTP and select the NTP servers to use to set the time. While you can set your system time manually, using NTP (Network Time Protocol) servers ensures your system time stays synchronized with Coordinated Universal Time (UTC). See Set the Conductor system time .
	Enter time manually	Check this box to set the time manually, and then enter the time, or select Set from browser time to use your browser's setting.
Configure email settings		These email settings are used to send messages from the Conductor for Airwall invitations, alerts and password resets. If you don't set these up, you will not be able to send or receive email from the Conductor.
Provision Conductor	Provision online or Provision offline	Provision your Conductor online by accessing the Tempered licensing servers. You need to be able to access licensing.temperednetworks.com on the Internet. If you're provisioning a dark Conductor, the wizard will walk you through the process.
Provision Conductor online	Voucher code	Enter the voucher code you received when purchasing your Conductor license.
	Use proxy server	Enable and enter your proxy server information if you need to go through a proxy server to access the Conductor licensing server.

Wizard page	Setting	Description
Provision Conductor offline		<p>Follow the steps to license your isolated (or "dark") Conductor offline:</p> <ol style="list-style-type: none"> 1. Generate a secure licensing request. 2. Send the licensing request to Tempered at support@tempered.io. 3. Import the encrypted licensing package you receive from Customer Success. <p>For more details, see License a Conductor and Airwall Edge Services in an Isolated Environment on page 164. If you get disconnected from the wizard during this step, it'll continue at the provisioning select screen. If that's the case, then select Provision Offline again and continue to the next step.</p>



Note: When you start up your Conductor, you'll have to proceed past the security warning (for example, in Firefox, click Advanced and then Accept risk). To avoid this warning, you can replace the Conductor-signed certificate with a custom certificate. See [Install a Custom CA Certificate Chain](#) on page 201.

Deploy a Physical Conductor

Tempered offers two physical Conductor models, the Conductor 400 Series and the Conductor 500 Series. Both are 1U rack-mount security appliances that facilitate private overlay networks between customer-provided equipment and devices.



Note: The hardware for an Conductor-500 and an Airwall Gateway-500 are similar. If your order contains both, check the bottom of the unit or the box for a sticker that marks Conductor hardware.



Note: For Conductor-500, use only Port 1 or Port 2. Do not connect anything to any of the other ports. For provisioning, and connection to the underlay network, connect to Port 1. For Diagnostics, connect to Port 2.

Familiarize yourself with your model's front panel layout, specifications, power requirements, and safety warnings before use. These can be found in your model's Platform Guide, included with your Conductor. If you are unable to locate your Platform Guide, you can download a PDF from the [Documentation Downloads](#) on page 649 Documentation Downloads section of Airwall help.

License and Provision a Conductor (v2.2.8 and earlier)

To get a Conductor up and running, you need license and provision it. You need your licensing voucher to complete these steps.

Supported Versions

Conductor v2.2.8 and earlier



Note: For v2.2.10 and later, licensing and provisioning is included in the Initial Conductor configuration wizard. Start at [Log in and Configure the Conductor](#) on page 169.

In v2.2.8 and earlier, you license the Conductor, and then [Log in and Configure the Conductor](#) on page 169.

1. If you have a physical Conductor, apply power to it, and connect a computer to Port 1 on the Conductor hardware using an Ethernet cable. Refer to your unit's Platform Guide for specific instructions.
2. In a web browser:

- **Physical Conductor** – go to: <https://192.168.56.2>
- **Cloud Conductor** – Click the link in your order email, or go to the public IP you set up when creating your Conductor.

The Conductor **Provisioning** page opens so you can license your Conductor.

3. If you have a proxy server between your Conductor and the Tempered licensing server, under **Disable network proxy settings**, configure proxy server settings to allow your Conductor to reach the licensing server.
4. If you are licensing an isolated (dark) Conductor, you will use the **Disable secure offline sync** section. For more details, see [License a Conductor and Airwall Edge Services in an Isolated Environment](#) on page 164.
5. In the **Voucher code** box, enter the voucher code you received from Tempered.
6. Click **Provision now**. It takes a moment to finish applying the voucher. Once complete, you should see the following:

7. Select [Click here to start using the Conductor](#).
8. [Log in and Configure the Conductor](#) on page 169.

Log in and Configure the Conductor

The first step in setting up a Conductor is to log in and configure it.

Before you begin

Before you begin, you will need the following:

- The IP or hostname of cloud or virtual Conductors. Follow the link in your order email, or go to the public IP you set up when creating your Conductor.
- Your Conductor license voucher code.

Set up a v2.2.10 or later Conductor

When you first set up a Conductor, it walks you through the initial configuration steps, then licensing and provisioning. For descriptions of the settings, see [Conductor Configuration Wizard Settings](#) on page 165.

1. If you have a physical Conductor, apply power to it, and connect a computer to Port 1 on the Conductor hardware using an Ethernet cable. Refer to your unit's Platform Guide for specific instructions.
2. In a web browser:
 - **Physical Conductor** – Go to: <https://192.168.56.2>
 - **Cloud Conductor** – Follow the link in your order email, or go to the public IP you set up when creating your Conductor.
 - **Virtual Conductor** – Go to <https://192.168.56.2>, or the IP address for Network adapter 1 or 2 that you set up when deploying your virtual Conductor.
3. Enter the default username (admin) and the password from your Tempered Order Delivery email, from your cloud provider (Tnw-<instance ID>, or the default password (admin123), and select **Sign in**.
4. Change your password when prompted, and select **Update**.
5. You're now in the Conductor Configuration Wizard. Follow the wizard to configure essential settings on your Conductor, and then license and provision it.

After provisioning is complete, accept the new Conductor certificate. Now you can [Add Airwall Edge Service Licenses to the Conductor](#) on page 160.



Note: When you start up your Conductor, you'll have to proceed past the security warning (for example, in Firefox, click Advanced and then Accept risk). To avoid this warning, you can replace the Conductor-signed certificate with a custom certificate. See [Install a Custom CA Certificate Chain](#) on page 201.

2.2.8 and earlier Conductor

With 2.2.8 and earlier, you need to [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160 first, then configure it.

1. In a browser window, enter the URL for your Conductor.
2. Enter the default username (admin) and the password from your Tempered Order Delivery email, from your cloud provider (usually Tnw-<instance ID>), or the default password (admin123), and select **Sign in**.
3. Change your password when prompted.
4. Select **Update**.
5. On the System Configuration dialog, you can leave all the fields as they are and select **Configure**. For recommended configuration, see [Best Practices for Conductor Configuration](#) on page 198.
6. Once configuration is finished, select **Return to settings**.

You should see the Conductor **Settings** page. You are now ready to connect Airwall Edge Services and devices, and create overlays.

Add Airwall Edge Service Licenses to the Conductor

The first step in licensing Airwall Edge Services is to add your licensing vouchers to the Conductor.

To add Airwall Edge Service licenses:

1. In Conductor, open **Settings**, and go to the **Licensing** tab.
2. Click **Enter Voucher**.
3. Type or paste your Voucher code, and click **Enter**. The licenses are added to your pool of licenses on the **Licensing** page.



Note: The Conductor automatically consolidates licensing vouchers.

Deploy a Conductor on a Cloud Platform

You can deploy a Tempered Conductor on several cloud platforms and manage physical, virtual, and cloud Airwall Edge Services and Airwall Agents.

Currently, you can deploy a Conductor on the following cloud platforms:

- Amazon Web Services (AWS)
- Microsoft Azure Cloud Platform
- Google Cloud Platform (GCP)
- [Amazon Web Services \(AWS\)](#)
- [Microsoft Azure Cloud Platform \(Azure\)](#)
- [Google Cloud Platform \(GCP\)](#)

There are several reasons you may choose to deploy your Conductor on a cloud platform:

- Conductor administrators can access a Conductor regardless of location.
- All three supported cloud platforms promise 99.9% up-time meaning that a Conductor will always be available and supported by each respective platform provider.
- Deploying a Conductor to the cloud reduces the risk associated with managing on-premises infrastructure, which can result in a significant cost savings over time.

If you decide to host your Conductor on a cloud platform, use the specific deployment instructions linked above for your chosen platform.

Deploy a Conductor on Alibaba Cloud

You can deploy an Airwall Conductor on Alibaba Cloud to manage physical, virtual, and cloud Airwall Edge Services, and Airwall Agents. Use the following steps to deploy a Conductor on Alibaba Cloud.

Supported Versions

Conductor 2.2.8 and later



Note: Click the print icon  at the top right of this topic to print or create a PDF.

Before you Begin

Before you begin, you need:

- Access to an Alibaba Cloud account. If you don't have an account, you can create one [here](#).
- Billing information set up for your Alibaba Cloud account.
- A Conductor license voucher. You need to purchase a voucher to license and log in to your Conductor once you've deployed it on Alibaba Cloud.



Note: See Alibaba Cloud for details and up to date instructions.

Step 1: Set up a Security Group

Before you start setting up the Conductor, you need to set up a Security Group and Networks in Alibaba Cloud for the Conductor.

1. Follow the instructions on Alibaba Cloud to log in to your account.
2. In Alibaba Cloud, on the **Elastic Compute Service** side menu, go to **Networks and Security**, then **Security Groups**.

3. Create a new Security Group for your Conductor, and set up the following **Inbound Security Group Rules**:
 - a) Allow ICMP IPv4 access. This allows the Conductor to check network communication and reachability (for example, ping).
 - b) Allow TCP on port 8096. This is the port the Conductor uses to communicate.
 - c) Allow TCP on 443/443. This opens up https:// for the Conductor's web interface and API calls.

Action	Protocol Type	Port Range	Authorization Type (All)	Authorization Object	Description	Priority
Allow	All ICMP (IPv4)	-1/-1	IPv4 CIDR Block	0.0.0.0/0	-	1
Allow	Custom TCP	8096/8096	IPv4 CIDR Block	0.0.0.0/0	-	1
Allow	Custom TCP	443/443	IPv4 CIDR Block	0.0.0.0/0	-	1

Step 2: Set up Networks

1. In Alibaba Cloud, on the Elastic Compute Service side menu, go to **Networks and Security**, then **VPCs**.
2. Create a VPC for your Conductor.
3. Set up 2 subnets in that network, and select the datacenter and zone for them (these need to be the same as you choose for the Conductor in the next step):
 - public_network
 - private_network

Now you're ready to set up the Conductor.

Step 3: Set up a Conductor in Alibaba Cloud

Set General Settings

1. Search for **Tempered Airwall Conductor** in the Alibaba Cloud marketplace.
2. Select **Choose Your Plan**.
3. Select your **Billing method** and **Region**. Make sure you choose the same datacenter and zone as the subnets you set up earlier.
4. For **Instance Type**, select `ecs.g5.large`.
5. For **Image**, leave it on the default Marketplace image.
6. Under **Storage**, set:
 - a) **System Disk** - Set to Ultra Disk with the minimum storage of 40 GiB.
 - b) **Data Disk** – Add a second Enhanced SSD drive with 120 GiB for the database and log files.
7. Select **Next: Networking** at the bottom to continue.

Set Networking Settings

8. Under **Network Type**:
 - a) **Type** - Choose VPC.
 - b) **Select a VPC** - Select the VPC network you set up earlier
 - c) **Select a VSwitch** – Select the public_network subnet you set up earlier.
9. Under **Public IP Address**, check the **Assign Public IP Address** box.
10. Under **Bandwidth Billing**, select **Pay by Traffic**.
11. Under **Security Group**, select the security group you created earlier.
12. Leave the rest of the settings as the default, and select **Next: System Configurations**.
13. For **Logon Credentials**, select **Set Later**.

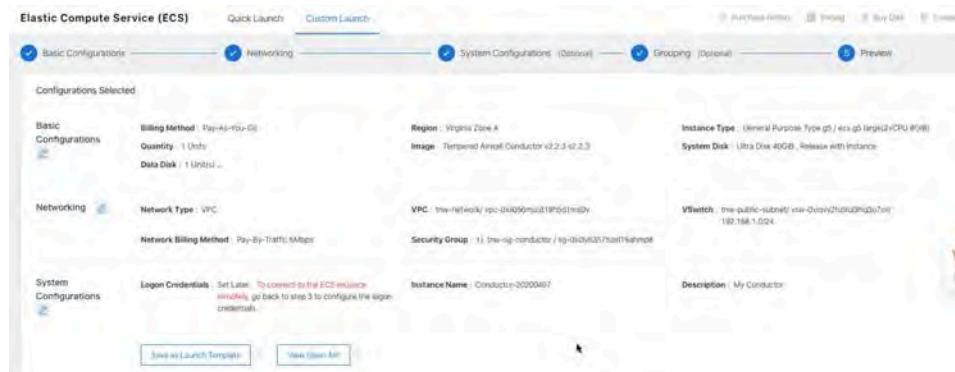
14. For **Instance Name**, set to Conductor-<date>. For example, Conductor-20200501.

15. (Optional) Fill in the **Description**, and set a **Hostname** if you have it set up.

16. Select **Next: Grouping**, then **Next: Preview**. (You do not need to set any Grouping settings.)

Preview your Settings and Create

17. On the **Preview** page, check your settings, check to accept the terms of service, and then select **Create Instance**.



You get a confirmation that your instance has been created.

18. Click **Console** to go to your Conductor instance page, where you can see the status of the instance being created.

Under IP address, note the IP of your Conductor.

Step 4: (Optional) Assign a permanent IP to your Conductor

If needed, you can assign a permanent IP address under Networks & Security, EIP. See the Alibaba Cloud help for instructions.

Verify, Configure, Provision, and License a Cloud Conductor

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see [Log in and Configure the Conductor](#) on page 169.



Note: In v2.2.8 and earlier, it shows the Provisioning page. See [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Here are the default passwords for cloud Conductors. You are prompted to change the password as soon as you log in:

- **Alibaba Cloud** – Tnw-<instanceID>
- **Amazon Web Services** – Tnw-<instanceID>
- **Microsoft Azure** – Tnw-<privateIpOfPublicNic>
- **Google Cloud** – Tnw-<instanceID>



Note: In Microsoft Azure, if you do not see a password on the Azure Outputs page next to **conductorPassword**, it's likely you are not using the Managed image.



Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

For more information, see:

- **Conductor v2.2.8 and earlier only** – [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160
- [Log in and Configure the Conductor](#) on page 169
- [Add Airwall Edge Service Licenses to the Conductor](#) on page 160
- [Conductor Configuration Wizard Settings](#) on page 165

Conductor v2.2.8 and earlier – Set Conductor System Time

After you've finished provisioning and licensing your v2.2.8 or earlier Alibaba Cloud Conductor, you may need to change the system time, as the default time zone may be out of sync with your current time. In v2.2.10 and later, you are prompted to set the system time during initial configuration.

1. In your Conductor, go to **Settings**.
2. Under System time, select **Edit Settings**.
3. Select **Set browser time**, and then select **Update**.

You can also enable NTP servers to set the system time. See **Set the Conductor system time** in Airwall help or your Airwall Deployment Guide.

You can also enable NTP servers to set the system time. See [Set the Conductor system time](#) on page 198.

Deploy a Conductor on Amazon Web Services (AWS)

You can deploy an Airwall Conductor on AWS and manage physical, virtual, and cloud Airwall Edge Services, and Airwall Agents. Use the following steps to deploy a Conductor on the AWS platform.



Note: Click the print icon  in the top right to print or download this topic.

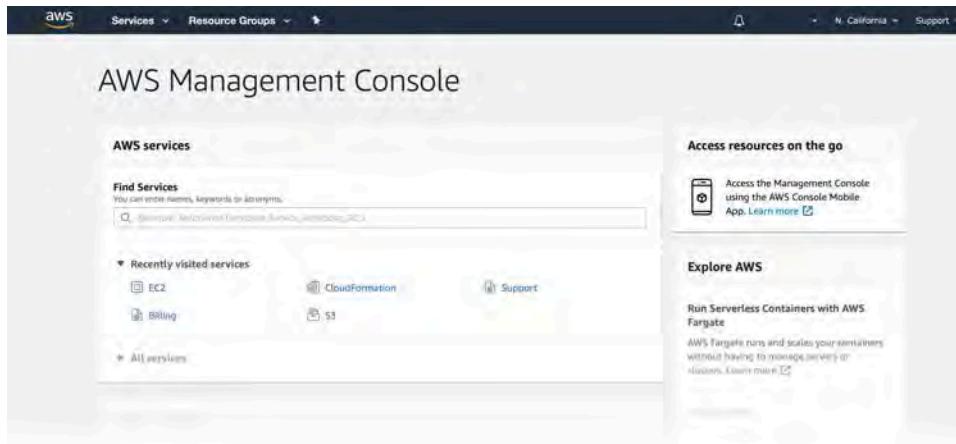
Prerequisites

To get started, you need to have:

- Access to a Amazon Web Services (AWS) account. If you don't have an account, you can create a free [AWS Free Tier](#) account and upgrade it to a full account later.
- Billing information set up on your AWS account. You cannot create a project until you are able to link your billing information to your newly created project.
- A Conductor license voucher if you want to start the Conductor and verify it is set up correctly. Fulfillment will provide this to you in an email after your purchase is complete.
- The Amazon Machine Image (AMI) ID that you received from Tempered Fulfillment when you purchased your AWS Conductor.

Log in to AWS

From a Web browser, navigate to <https://console.aws.amazon.com/> and log in to your account to get to the AWS Management Console, pictured below:



Create a Launch Instance

When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including Amazon EC2. You add the Tempered Conductor as an EC2 instance, so make sure you have the AMI ID that you received from Tempered Fulfillment when you purchased your AWS Conductor.

To create an instance:

- On the top bar of the **AWS Management Console**, select **Services** and then select **EC2** to access the **EC2 Dashboard**.

- In the **Create Instance** section, click **Launch Instance**.

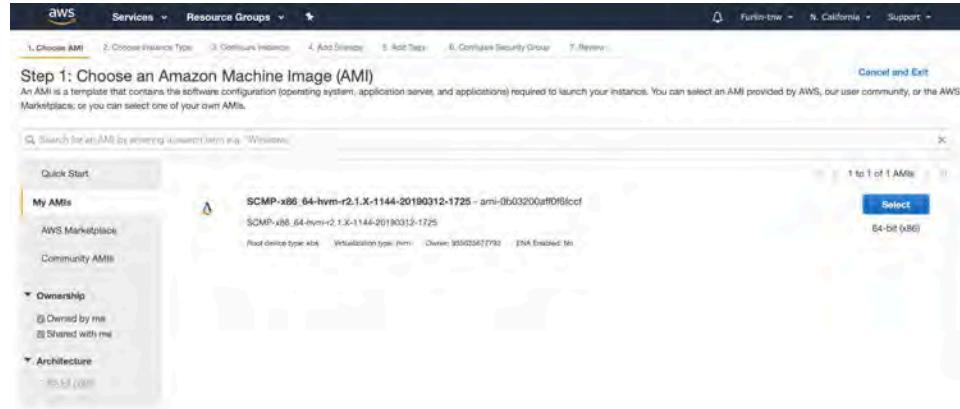
- Click **Launch Instance** to start the instance setup wizard.

Step 1: Choose an Amazon Machine Image (AMI)

The AMI is a custom template used to create a Conductor as a virtual machine in AWS. It contains the Conductor's root volume, permissions, and device mappings necessary to deploy the Conductor to your account.

- On the **Choose AMI** tab, click **My AMIs** on the left.

2. Under **Ownership**, check the **Shared with me** box. You should see the Conductor image listed in the right pane.



3. Click the **Select** button on the right to continue.

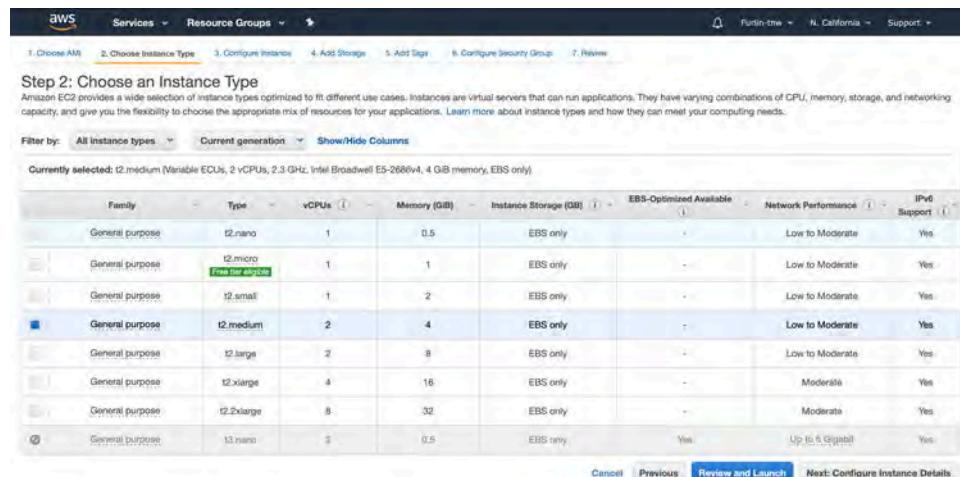
Step 2: Choose an Instance Type

The Amazon EC2 instance type identifies the combination of memory, networking capacity, CPU, and storage required by an application. For the Conductor we recommend a minimum machine type of **t2.medium**.

1. On the **Choose Instance Type** tab, select your desired instance type and click **Next: Configure Instance Details**.



Important: DO NOT select the **Review and Launch** button, as this option will use the default settings for this instance type. You will need to make changes for the Conductor to operate correctly.



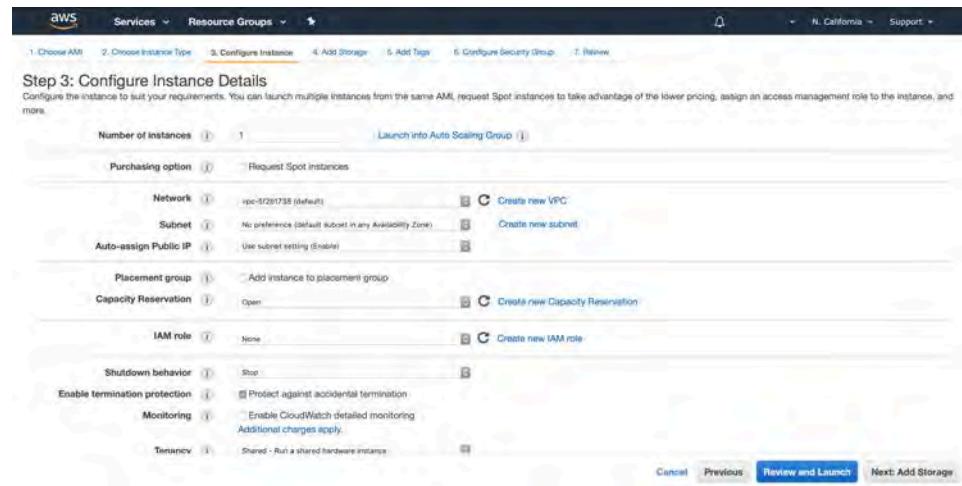
2. Click **Next: Configure Instance Details** to continue.

Step 3: Configure Instance Details

Your new instance requires that you to make a few changes to ensure the Conductor has access to resources needed for proper operation. Make the following changes as outlined below.

1. On the **Configure Instance** tab, do the following:
 - a) Select your desired VPC from the **Network** drop-down.
 - b) Select your region from the **Subnet** drop-down.
 - c) Select **Enable termination protection** (recommended)

You can leave all other settings as is.



2. Click **Next: Add Storage** to continue.

Step 4: Add Storage

The Conductor AMI supplied by Tempered is relatively small in size. The configuration information and storage, however, requires a second hard disk, which you set up as part of the instructions below.

1. On the Add Storage tab, click **Add New Volume**.



Note: The volume must be a minimum of 32 GB. This size should be sufficient for normal operation; however, you can resize your volume later should you require additional space. See [Modifying the Size, Performance, or Type of an EBS Volume](#) in the AWS documentation for more information.

2. Change the following information on the new volume:

- a) Select **/dev/sdf** from the **Device** drop-down.



Important: We recommend you use **/dev/sdf** for your second volume. Do not select /dev/sdb, /dev/sdc, or /dev/sdd as the Conductor will not function correctly. Other partitions may work but are not currently supported.

- b) Enter the value **32** in the **Size (GiB)** field.
- c) Check **Delete on Termination**.

You can leave all other settings as is.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snelp-03e898d5c8d00754	1	Magnetic (standard)	N/A	N/A	<input checked="" type="checkbox"/>	Not Encrypted
ebs	/dev/sdc	(Select (empty))	32	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB. Set my root volume to General Purpose (SSD).
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

3. Click **Next: Add Tags** to continue.

Step 5: Add Tags

Tagging your Conductor instance can help you identify it if you have a large number of instances deployed to your account. While not required, we recommend you add a tag so you can find it quickly.

1. On the **Add Tags** tab, click **Add Tag** and enter the following:

- a) Enter **Name** in the **Key** column.
- b) Enter a name for your Conductor in the **Value** column.

Key	Value	Instances	Volumes
Name	Tempered Conductor	<input type="checkbox"/>	<input type="checkbox"/>

Add another tag (Up to 50 tags maximum)

2. Click **Next: Configure Security Group** to continue.

Step 6: Configure Security Group

Configuring a security group is synonymous with configuring firewall rules. You need to add three rules: ICMP to allow Airwall Edge Services to validate their link to the Conductor, HTTPS to allow for Conductor management, and a custom rule to allow Airwall Edge Services to communicate with the Conductor on port 8096.

1. In the **Assign a security group** section, select the **Create a new security group** radio button.
2. In the **Security group name** field, enter a name for your security group.
3. In the **Description** field, enter a description for your security group, or leave the default.
4. Add three rules to your security group:
 - a) Click **Add Rule**, select **All ICMP – IPv4** from the **Type** drop-down, select **Anywhere** from the **Source** drop-down, and enter **ICMP** in the **Description** column.
 - b) Click **Add Rule**, select **HTTPS** from the **Type** drop-down, select **Anywhere** from the **Source** drop-down, and enter **SSL** in the **Description** column.
 - c) Click **Add Rule**, select **Custom TCP Rule** from the **Type** drop-down, enter **8096** in the **Port Range** column, select **Anywhere** from the **Source** drop-down, and enter **MAP** in the **Description** column.

Type	Protocol	Port Range	Source	Description
All ICMP - IPv4	ICMP	0 - 8096	Anywhere	ICMP
HTTPS	TCP	443	Anywhere	SSL
Custom TCP Rule	TCP	8096	Anywhere	MAP

Warning: You will not be able to connect to this instance as the AMI requires port(s) 22 to be open in order to have access. Your current security group doesn't have port(s) 22 open.

Warning: Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel **Previous** **Review and Launch**

5. Click **Review and Launch** to continue.



Note: If you receive a **Boot from General Purpose (SSD)** dialog, select the **Continue with Magnetic as the boot volume for this instance** radio button and then click **Next**.

Step 7: Review

1. Review your setup information and if everything is correct, click **Launch**.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

SCMP-x86_64-hvm-r2.1.X-1144-20190312-1725 ~ ami-0b03200aff0ffccf
SCMP-x86_64-hvm-r2.1.X-1144-20190312-1725

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.medium	Variable	2	4	EBS only	-	Low to Moderate

Security Groups

Tempered Conductor SG
Description: launch-wizard-1 created 2019-04-03T10:44:31.385-07:00

Cancel **Previous** **Launch**

2. In the **Select an existing key pair or create a new key pair** dialog, create a new key pair or enter one of your existing key pairs.



Note: This keypair is required to complete the wizard, but is never used since SSH is not enabled on Conductors.

3. Click **Launch Instance**.

Verify, Configure, Provision, and License a Cloud Conductor

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see [Log in and Configure the Conductor](#) on page 169.



Note: In v2.2.8 and earlier, it shows the Provisioning page. See [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Here are the default passwords for cloud Conductors. You are prompted to change the password as soon as you log in:

- **Alibaba Cloud** – Tnw-<instanceID>
- **Amazon Web Services** – Tnw-<instanceID>
- **Microsoft Azure** – Tnw-<privateIpOfPublicNic>
- **Google Cloud** – Tnw-<instanceID>



Note: In Microsoft Azure, if you do not see a password on the Azure Outputs page next to **conductorPassword**, it's likely you are not using the Managed image.



Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

For more information, see:

- **Conductor v2.2.8 and earlier only** – [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160
- [Log in and Configure the Conductor](#) on page 169
- [Add Airwall Edge Service Licenses to the Conductor](#) on page 160
- [Conductor Configuration Wizard Settings](#) on page 165

Additional Information

Once your Conductor is installed, you can configure and manage it as you would a physical Conductor. See [Configure a Conductor](#) on page 198. For additional help, you can access search **Airwall help** by using the search bar at the top of the page or the navigation links to the left.

Deploy a Conductor on Microsoft Azure

You can deploy an Airwall Conductor on Azure and manage physical, virtual, and cloud Airwall Edge Services, and Airwall Agents. Use the following steps to deploy a Conductor on the Microsoft Azure platform.



Note: Click the print icon  in the top right to print or download this topic.

Prerequisites

To get started, make sure you have access to your Azure account. If you don't have an account, you can create a free [Microsoft Azure](#) account and upgrade it to a full account later. If you have an existing Azure account, make sure your billing information is set up. You cannot create a project until you are able to link your billing information to your newly created project.

You need to purchase a Conductor license voucher for your Conductor to complete Step 3. After your purchase is complete, you get an email from Tempered Fulfillment with your voucher code.



Note: If you are familiar with how Azure organizes the components, you should be able to easily understand what is required and create them manually. However, this document does not cover a full manual deployment of a Conductor in Azure.

Step 1: Log in to Azure Cloud

From a Web browser, navigate to <https://portal.azure.com> and log in using your Azure credentials.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with navigation links like Home, Dashboard, All services, Favorites (All resources, Resource groups, Quickstart Center, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing), and Create a resource. The main area has a header "Azure services See all (100+)" with icons for Virtual machines, Storage accounts, App Services, SQL databases, Azure Database for PostgreSQL, Azure Cosmos DB, Kubernetes services, and Function App. Below this are cards for Microsoft Learn, Azure Monitor, Security Center, and Cost Management. A "Recent resources" section lists "Pay-As-You-Go" as a Subscription viewed 8 min ago. To the right, there's a "Useful links" section with links to Technical docs, Azure products, Azure latest updates, and Azure blog. At the bottom, there are download links for the Azure mobile app on the App Store and Google Play.

Step 2: Add a Conductor image

You add a Conductor image from the Azure marketplace to your project to create an instance.

1. In Azure, select **Create a Resource**, and search for Tempered Conductor Deployment.
2. Select **Tempered Airwall Conductor Deployment Wizard 2.2**, go to the **Plans** tab and check the version of the Conductor, and then select **Create**.

The screenshot shows the Azure Marketplace listing for the "Tempered Airwall Conductor Deployment Wizard v2.2". It features a yellow shield logo, the product name, developer information ("By Tempered Networks, Inc"), a description ("Tempered Airwall Conductor Orchestration Engine Deployment Wizard version 2.2"), a price indicator ("Price varies"), and a "Get it now" button.

3. On the Create Tempered Airwall Conductor Managed 2.2 page, **Basics** tab:

Subscription

Select your subscription model from the drop-down.

Resource group

Create a resource group for your virtual network. To do this click **Create New**, enter a new name, and click **OK**.

Region

Select the region for this instance.

4. Select **Next: Virtual Machine Settings**. On the **Virtual Machine settings** tab:

Virtual Machine name

Enter a prefix for the virtual machine.

Configure virtual networks

Select or create a Virtual network.

Public shared subnet

Select a public subnet from the virtual network you selected.

5. Select **Next: Endpoint settings**. On the Endpoint Settings page:

Conductor Public IP address

Select **Create new**, then under **Create public IP address**, set **SKU** to **Basic** and **Assignment** to **Static**, and select **OK**.

DNS label

Enter a prefix for the DNS name. Check to make sure you get the green check, indicating the name is valid.

6. Select Next: Review + create.

7. Review your settings, and accept the Terms of Use, and then select **Create**. Azure starts deploying your image to the resource group you specified.

Basics	
Subscription	Pay-As-You-Go
Resource group	00tn-conductor
Region	West US

Virtual Machine settings	
Virtual machine name prefix	tnconductor
Virtual machine size	Standard_A2_v2
Virtual network	vnet01
Public shared subnet	publicSubnet
Address prefix (Public shared subnet)	10.3.0.0/24
Virtual machine data volume size	120
Virtual machine data volume type	Standard_LRS

Endpoint settings	
Public IP address	ip01
Domain name label	tn-demo-conductor

Step 3: Verify the install

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see [Log in and Configure the Conductor](#) on page 169.



Note: In v2.2.8 and earlier, it shows the Provisioning page. See [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.



Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

1. When Azure finishes deploying, it takes you to the Conductor instance. Leave this page up as you verify the install. Navigate to **Outputs**, and next to **publicIp**, select the copy icon to copy the public IP for your cloud Conductor.
2. Go to a web browser, enter in the IP you copied, and bypass the security warning.
3. Sign in to the Conductor:
 - a) Go back to Azure Outputs page, and next to **conductorPassword**, click the copy icon to copy the Conductor password.



Note: If you do not see a password on this page, it's likely you are not using the Managed image.

- b) Enter username: `admin`, and the password you copied. The default is `Tnw-<privateIpOfPublicNic>`.
- c) Change your password when prompted.

4. The Conductor starts the Initial Conductor Configuration wizard. To log in, configure, and license your Conductor, see [Log in and Configure the Conductor](#) on page 169.



Note: In v2.2.8 and earlier, it shows the Provisioning page. See [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160.

5. When you've finished configuring, licensing, and provisioning your Conductor, you can sign in to start using or continuing configuring your Conductor.

For more information, see:

- [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160
- [Log in and Configure the Conductor](#) on page 169
- [Add Airwall Edge Service Licenses to the Conductor](#) on page 160
- [Conductor Configuration Wizard Settings](#) on page 165

Verify, Configure, Provision, and License a Cloud Conductor

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see [Log in and Configure the Conductor](#) on page 169.



Note: In v2.2.8 and earlier, it shows the Provisioning page. See [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Here are the default passwords for cloud Conductors. You are prompted to change the password as soon as you log in:

- **Alibaba Cloud** – `Tnw-<instanceID>`
- **Amazon Web Services** – `Tnw-<instanceID>`
- **Microsoft Azure** – `Tnw-<privateIpOfPublicNic>`
- **Google Cloud** – `Tnw-<instanceID>`



Note: In Microsoft Azure, if you do not see a password on the Azure Outputs page next to **conductorPassword**, it's likely you are not using the Managed image.



Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

For more information, see:

- **Conductor v2.2.8 and earlier only** – [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160
- [Log in and Configure the Conductor](#) on page 169
- [Add Airwall Edge Service Licenses to the Conductor](#) on page 160
- [Conductor Configuration Wizard Settings](#) on page 165

Additional Information

Once your Conductor is installed, you can configure and manage it as you would a physical Conductor. See [Configure a Conductor](#) on page 198. For additional help, you can search **Airwall help** by using the search bar at the top of the page or the navigation links to the left.

Deploy a Conductor on the Google Cloud Platform (GCP)

You can deploy an Airwall Conductor on GCP and manage physical, virtual, and cloud Airwall Edge Services, and Airwall Agents. Use the following steps to deploy on the Google Cloud platform.



Note: Click the print icon  in the top right to print or download this topic.

Prerequisites

To get started, make sure you have access to your Google Cloud account. If you don't have an account, you can create a free [Google Cloud](#) account and upgrade it to a full account later. If you have an existing Google Cloud account, make sure your billing information is set up. You cannot create a project until you are able to link your billing information to your newly created project.



Note: You should be familiar with using Google Cloud before attempting to deploy a Tempered Conductor or Airwall Gateway on the platform. To get started, we recommend you review the following content offered by Google:

- [Google Cloud Platform Overview](#)
- [Google Cloud Storage](#)
- [Virtual Private Cloud](#)
- [Google Compute Engine Documentation](#)

A Conductor license voucher is necessary at the end of this procedure if you want to start the Conductor and verify it is set up correctly. Fulfillment will provide this to you in an email after your purchase is complete.

Step 1: Log in to Google Cloud

From a Web browser, navigate to <https://console.cloud.google.com>. You will see one of two pages, the **Getting Started** page if you have no projects or the **Home** page if you have existing projects.

Step 2: Create and configure a project

A Google Cloud project organizes all of your resources into a logical group for easier management. You will add the Tempered Conductor to a new or existing project, so you need to have a project created before you deploy the Conductor.



Note: If you are adding the Conductor to an existing project, you can skip step 2 and proceed directly to step 3 in this document.

1. On the top bar of the Google Cloud page, click **Select a project**.



2. On the upper-right corner of the Select a project dialog, click **New Project**.



3. In the **Project Name** field, enter a name for your new project. By default, your new project is assigned a default ID, which you can change by clicking **Edit** to the right of the **Project ID** field.
4. Optional: If you want to add your project to an organization you have already created, select it in the **Location** field by clicking **Browse** to the right. For more information about organizations, see [Quickstart Using Organizations](#) in the Google Cloud documentation.

The screenshot shows the 'New Project' dialog. It includes a quota warning message: 'You have 22 projects remaining in your quota. Request an increase or delete projects.' with a 'Learn more' link and a 'MANAGE QUOTAS' button. The 'Project name *' field contains 'My Project 43972'. The 'Project ID *' field contains 'liquid-fuze-235914' with a 'C' icon for edit. Below it is a note: 'Project ID can have lowercase letters, digits, or hyphens. It must start with a lowercase letter and end with a letter or number.' The 'Location *' field shows 'No organization' with a 'BROWSE' button. Below it is a note: 'Parent organization or folder'. At the bottom are 'CREATE' and 'CANCEL' buttons.

5. Once you are finished, click **Create**.

It will take a moment to set up your project. A notification window will indicate when the operation is complete. You can then select **Home** in the Google Cloud sidebar to access your dashboard.

Step 3: Set up firewall rules

GCP firewall rules will manage the traffic coming into your instance on a network. By default, you have a network with a default set of firewall rules for your region, and you will need to make a few changes to set up your environment so the Conductor can function correctly.



Note: This step assumes you are using the default network for your region. If you would like to create a separate virtual private cloud (VPC) network, please review the topic [Virtual Private Cloud \(VPC\) Network Overview](#) in the Google Cloud documentation.

To set up firewall rules:

- In the Google Cloud sidebar, navigate to the **Networking** section, hover over **VPC network**, and select **Firewall rules**.

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default
default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp 0-65535 udp 0-65535 icmp	Allow	65534	default
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp 3389	Allow	65534	default
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp 22	Allow	65534	default

- Click **Create Firewall Rule**.

Firewall rules **CREATE FIREWALL RULE** **REFRESH** **DELETE**

- Fill in the **Create firewall rule** page with the following information:

Name

You can use any name you choose, but it must be lowercase with no spaces.

Description

This can be anything you like. We recommend something descriptive such as **Firewall access rules for Tempered Conductor**.

Network

Select **default** from the drop-down unless you are using a different network.

Direction of traffic

Select the **Ingress** radio button.

Action on match

Select the **Allow** radio button.

Targets

Select Specific target tags from the drop-down.

Target tags

Enter **tempered-conductor-rules**



Note: Remember this tag. You will need it later in this procedure.

Source filter

Select **IP ranges** from the drop-down.

Source IP ranges

Enter **0.0.0.0/0**.

Protocols and ports

Select the **Specified protocols and ports** radio button and enter **443,8096**.



Note: Do not check the box next to **tcp** and then select the field to enter your ports – the box will revert to unchecked and disable both fields. Click only on the field to enter your ports.

Leave all other fields as is.

Your page should look similar to the image below:

[←](#) Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Name

Description (Optional)

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more
 On
 Off

Network

Priority Priority can be 0 - 65535 Check priority of other firewall rules

Direction of traffic
 Ingress
 Egress

Action on match
 Allow
 Deny

Targets

Target tags

Source filter

Source IP ranges

Second source filter

Protocols and ports
 Allow all
 Specified protocols and ports
 tcp :
 udp :
 Other protocols

Disable rule

Create **Cancel**

Equivalent REST or command line

4. Click **Create**. It will take a moment to finish the operation. Once complete, you should see the following in your rules list:

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network
tempered-conductor	Ingress	tempered-conductor-rules	IP ranges: 0.0.0.0/0	tcp:443,8096	Allow	1000	default

Step 4: Add a Conductor Image

Add a Conductor image to create an instance in your Google Cloud project.

To add an image:

1. In the Google Cloud sidebar, navigate to the **Compute** section, hover over **Compute Engine**, and select **Images**.

Name	Size	Created by
c0-deeplearning-common-cu100-20190312	30 GB	c0-deeplearning-common-
c1-deeplearning-pytorch-1-0-cu100-20190314	30 GB	c1-deeplearning-pytorch-1
c2-deeplearning-tf-1-13-cu100-20190314	10 GB	c2-deeplearning-tf-1-13-cu
centos-6-v20190326	10 GB	CentOS
centos-7-20190213	10 GB	CentOS
centos-7-v20190326	10 GB	CentOS
coreos-alpha-2093-0-0-v20190326	9 GB	CoreOS
coreos-beta-2079-1-0-v20190326	9 GB	CoreOS
coreos-stable-2023-5-0-v20190312	9 GB	CoreOS
cos-69-10895-172-0	10 GB	Google
cos-73-11647-112-0	10 GB	Google
cos-beta-74-11895-32-0	10 GB	Google

2. Click **Create Image**.



3. Fill in the **Create an image** page with the following information:

Name	Enter conductor-r216-1144 .
Description	Enter Tempered Conductor version 2.1.6 .
Source	Select Cloud Storage file from the drop-down.
Cloud Storage File	Enter tempered-image-storage/conductor-r216-1144.tar.gz .

You can leave all other fields as they are.

4. Click **Create**. It will take a moment to finish the operation.

Once complete, you should see the following in your images list:

Name	Size	Created by
conductor-r216-1144	1 GB	My New Project

 **Note:** If you have multiple projects, make sure the image is associated with your desired project, listed in the **Created by** column.

Step 5: Create a Conductor Instance

The Conductor image can now be used to create a virtual machine instance. The image supplied by Tempered contains the Conductor and is relatively small in size. Configuration information and storage requires a second hard disk, which you will set up as part of the instructions below. This image must be a minimum of 120 GB.

To create a Conductor instance:

- Select the image in the list by clicking on its name. You have several options available: Select **Create Instance**.

conductor-r216-1144

Labels
None

Creation time
Mar 28, 2019, 1:37:23 PM

Encryption type
Google managed

[Equivalent REST](#)

- Fill in the **Create an instance** page with the following information:

Name Enter a name of your choice, but it must be lower case and without spaces.

Region Select the region of your choice from the drop-down.

Zone Select the zone of your choice from the drop-down.

You can leave all other fields as is.

Name tempered-conductor

Region us-west1 (Oregon) **Zone** us-west1-b

Machine type
Customize to select cores, memory and GPUs.
1 vCPU 3.75 GB memory Customize
Upgrade your account to create instances with up to 96 cores

Container
Deploy a container image to this VM instance. [Learn more](#)

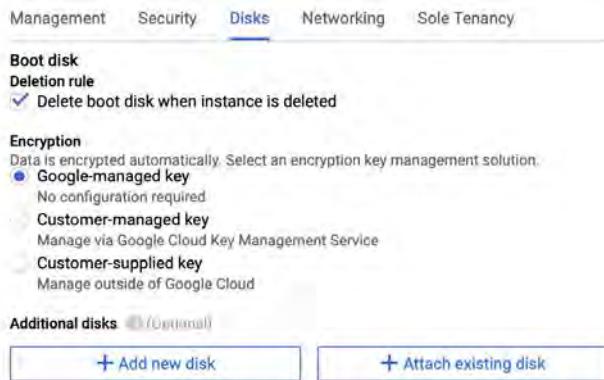
Boot disk
New 1 GB standard persistent disk
Image conductor-r216-1144 Change

Identity and API access
Service account: Compute Engine default service account
Access scopes:
Allow default access
Allow full access to all Cloud APIs
Set access for each API

Firewall
Add tags and firewall rules to allow specific network traffic from the Internet
Allow HTTP traffic Allow HTTPS traffic
Management, security, disks, networking, sole tenancy

- Click **Management, security, disks, networking, sole tenancy**.

4. On the **Disks** tab, leave all settings as is and click **+ Add new disk**.



5. In the **New disk** dialog enter the following:

Name	You can leave this field as disk 1 , otherwise enter a name of your choice.
Type	Select Standard persistent disk from the drop-down.
Source type	Select Blank disk .
Deletion rule	Select the Delete disk radio button

Size (GB)Enter the value **200**

You can leave all other settings as is.

New disk (disk-1, Blank, 200 GB)

Name (Optional)	disk-1	
Description (Optional)		
Type	Standard persistent disk	
Source type	<input checked="" type="radio"/> Blank disk <input type="radio"/> Image	
Mode	<input checked="" type="radio"/> Read/write <input type="radio"/> Read only	
Deletion rule	When deleting instance <input checked="" type="radio"/> Keep disk <input type="radio"/> Delete disk	
Size (GB)	200	
Estimated performance		
Operation type	Read	Write
Sustained random IOPS limit	150.00	300.00
Sustained throughput limit (MB/s)	24.00	24.00
Encryption		
Data is encrypted automatically. Select an encryption key management solution.		
<input checked="" type="radio"/> Google-managed key No configuration required. <input type="radio"/> Customer-managed key Manage via Google Cloud Key Management Service <input type="radio"/> Customer-supplied key Manage outside of Google Cloud		
This new disk will be added once you create the new instance.		
<input type="button" value="Done"/> <input type="button" value="Cancel"/>		

- Click **Done**. The dialog will close, and you should see the following:

Additional disks (Optional)

New disk (disk-1, Blank, 200 GB)	<input type="button" value="Edit"/>
<input type="button" value="+ Add new disk"/>	<input type="button" value="+ Attach existing disk"/>

- Click the **Networking** tab to the right of the **Disk** tab and enter the tag name you created for your firewall rules in step 3.

- Click **Create**. It will take a moment to finish the operation. Once complete, you should see the following:

Filter VM instances							Columns ▾
Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect	
instance-1	us-east1-b			10.142.0.2 (nic0)	104.196.3.72	SSH	⋮



Note: The **External IP** for your instance is the address you will use to connect to the Conductor.

Verify, Configure, Provision, and License a Cloud Conductor

At this point the Conductor instance is running in your cloud provider.

To verify, paste your Conductor IP into a browser window. It should show you the Initial Conductor Configuration page. To log in, configure, and license your Conductor, see [Log in and Configure the Conductor](#) on page 169.



Note: In v2.2.8 and earlier, it shows the Provisioning page. See [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160.

It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.

Here are the default passwords for cloud Conductors. You are prompted to change the password as soon as you log in:

- Alibaba Cloud** – Tnw-<instanceID>
- Amazon Web Services** – Tnw-<instanceID>
- Microsoft Azure** – Tnw-<privateIpOfPublicNic>
- Google Cloud** – Tnw-<instanceID>



Note: In Microsoft Azure, if you do not see a password on the Azure Outputs page next to **conductorPassword**, it's likely you are not using the Managed image.



Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a custom certificate on the Conductor that prevents these notifications in the future.

For more information, see:

- Conductor v2.2.8 and earlier only** – [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160
- [Log in and Configure the Conductor](#) on page 169
- [Add Airwall Edge Service Licenses to the Conductor](#) on page 160
- [Conductor Configuration Wizard Settings](#) on page 165

Additional Information

Once your Conductor is installed, you can configure and manage it as you would a physical Conductor. See [Configure a Conductor](#) on page 198. For additional help, you can access search **Airwall help** by using the search bar at the top of the page or the navigation links to the left.

Conductor for Google Cloud Platform Quick Start

To get started, make sure you have access to your Google Cloud account. If you don't have an account, you can create a free [Google](#) Cloud account and upgrade it to a full account later. If you have an existing Google Cloud account, make sure your billing information is set up. You cannot create a project until you are able to link your billing information to your newly created project.

A Conductor license voucher is necessary at the end of this procedure if you want to start the Conductor and verify it is set up correctly. Fulfillment will provide this to you in an email after your purchase is complete.

Step 1: Log in to Google Cloud

From a Web browser, navigate to <https://console.cloud.google.com>. You will see one of two pages, the **Getting Started** page if you have no projects or the **Home** page if you have existing projects.

Step 2: Select the Tempered Conductor from the Marketplace

Select the Conductor in the Google Cloud Marketplace.

1. From your GCP Dashboard, select **Marketplace** on the left sidebar.
2. In the **Search** field at the top of the page, enter **tempered networks conductor** and press enter.
3. In the results list, locate and select **Tempered Networks Conductor v2.1**.

The product page opens where you can deploy the Conductor.

Step 3: Install the Conductor Image

1. On the product page, click **LAUNCH ON COMPUTE ENGINE**.
2. The Conductor deployment uses a template so most settings you can leave as is, however you may want to make the following changes:
 - a) **Deployment name:** Enter a name for your Conductor.
 - b) **Zone:** Select a zone from the drop-down. The zone determines what computing resources are available and where your data is stored and used.
 - c) **Machine type:** Leave as is. Machine type determines the amount of memory, virtual cores, and persistent disk limits for the Conductor. The default settings are required for the Conductor to function correctly.
 - d) **Data Disk:** Leave the **Data disk type** and **Data disk size in GB** fields as is.
 - e) **Networking:** Leave the **Network**, **Subnetwork**, **External IP**, **Firewall**, and **IP forwarding** fields as is.



Note: Some fields may be hidden based on your screen size. To view these fields, click **More** just above the **Deploy** button.

3. Click **Deploy**.

Step 4: Finalize the Deployment

It will take a few moments for the process to complete. You can view the progress of your deployment by viewing the tree hierarchy of your components on the page.

Once complete, the message changes indicating your deployment is complete.

Step 5: Obtain your Conductor Address and Credentials

When your Conductor finishes installing, its information appears in the right pane of the page. You need three pieces of this information to log in to your Conductor for the first time: your Conductor site address, username, and temporary password.

Conductor site address

Copy from **Site address**, or click **Visit the site** to open it in your browser.

Username and password

Copy from the shaded box near the bottom.

Tempered Networks Conductor v2.1

Solution provided by Tempered Networks

Site address	https://tempered-conductor-v21-1-vm.us-central1-f.n1-highcpu-2.computeengine.google.com
Instance	tempered-conductor-v21-1-vm
Instance zone	us-central1-f
Instance machine type	n1-highcpu-2

[More about the software](#)

Get started with Tempered Conductor v2.1

[Visit the site](#)

Suggested next steps

- Request a license
This is a BYOL solution which requires a valid license to use. [Request a license](#)
- The temporary Conductor password
A temporary Conductor password has been assigned to the Conductor


Step 6: Verify the install

At this point the Conductor instance is running in Google Cloud. You should verify it is installed correctly by logging in and licensing the Conductor. It may take several minutes for the Conductor to become available after it starts, so if you attempt to access it and your browser appears to stop responding, please try again in a few minutes.



Note: When running the Conductor for the first time, you may receive notifications indicating the connection is not private. Once you have finished configuring the Conductor, you can install a customer certificate on the Conductor that prevent these notifications

To verify the install:

1. Point your web browser to the external IP address for your Conductor. Make sure you begin the address with <https://>.
2. An unlicensed Conductor will display the initial **Provisioning** page where you enter your license voucher.
3. Enter the voucher code you received from Tempered in the **Voucher code** field.
4. Click **Provision now**. It will take a moment to finish the operation. Once complete, you should see confirmation page.
5. Select **Click here to start using the Conductor**.
6. Enter the default username and password you received when you completed installation and click **Sign in**.
7. You will be prompted to enter a new password. Enter the default password in the **Current password** field and a new password of your choosing in the **New password** and **Confirm new password** fields.

8. Click **Update**.

9. On the System Configuration dialog, leave all the fields as is and click **Configure**.

10. It will take a moment to complete the operation. Once finished, click **Return to settings**.

You should see the Conductor **Settings** page. On the right side in the **Network adapter 1** section, the IP address should match the **Internal IP** of your instance in the GCP portal.

The screenshot shows the 'Configuration' page of the Airwall Conductor. At the top, there is a 'Setup' button. Below it, the 'Hostname' is listed as 'conductor'. The 'Firmware version' is '2.2.3'. The 'Serial number' is '42305592D699'. The 'Airwall Conductor device ID' is 'AMA@40130#42305592D699'. The main content area is divided into sections for 'Network adapter 1' and 'Network adapter 2'. Under 'Network adapter 1', it says 'Web access is enabled'. The 'IP address' is '172.16.126.122', 'Netmask' is '255.255.0.0', 'Default gateway' is '172.16.0.254', and 'DNS servers' is '8.8.8.8'. Under 'Network adapter 2', it also says 'Web access is enabled'. The 'IP address' is '10.126.10.122', 'Netmask' is '255.255.255.0'. At the bottom, there is a 'Proxy server settings' section with an 'Edit settings' button, which is currently set to 'Disabled'.

Deploy a Conductor in VMware ESX/ESXi

Prerequisites

- An existing installation of VMware ESX/ESXi server version 6.5.0 and later
- A VMware open virtual appliance (OVA) for a Conductor or Airwall Gateway.

System Requirements

The following VMware ESX/ESXi server hardware is required:

Processor

- Minimum requirement of a single processor with hyper-threading support, VT-x technology, and 64-bit architecture.
- Optimum configuration is minimum 4 processing cores with hyper-threading support, VT-x technology, 64-bit architecture, and AES-NI enabled in the host's BIOS.

Virtual image

Below are the minimum configuration requirements available for a virtual Conductor or Airwall Gateway image:

Platform	Memory	Disk
Conductor	4GB	120GB*
Airwall Gateway	1GB	1GB*

* Already included in the default OVA package

To deploy a virtual Conductor

1. Deploy a new OVF template from within vSphere or vCenter. For most deployments, the default settings are sufficient.
2. Browse to the location of the downloaded OVA file.
3. Give the virtual machine a unique name and select its storage location.
4. Map the virtual machine's network interfaces with the correctly assigned port groups for the Conductor.
5. Disk provisioning can be set to **Thin Provisioned**
6. Verify the configuration, check **Power on after deployment**, and then click **Finish** to begin the update.

To configure the Conductor

An unlicensed, new VMware Conductor deploys with the default configuration.

- Network adapter 1 is configured with a static IP address of 192.168.56.2
- Network adapter 2 is configured for DHCP IP addressing

To determine the IP address assigned to network adapter 2, at the console, log in with name: `airsh`, and password: `airsh`, and then type `status`.

Run the Conductor web UI on either of the network adapters. To continue:

- **For a v2.2.10 and later Conductors**, see [Log in and Configure the Conductor](#) on page 169.
- **For v2.2.8 or earlier Conductors**, see [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160.

For more information, see:

- [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160
- [Log in and Configure the Conductor](#) on page 169
- [Add Airwall Edge Service Licenses to the Conductor](#) on page 160

Deploy a Conductor in Microsoft Hyper-V

The virtualization server role for Windows Server 2012 R2 is called Hyper-V Manager. The following documentation show the steps to implement and manage a secure Airwall Gateway and overlay network on Hyper-V network.

Prerequisites:

- An existing installation of Microsoft Hyper-V, v2012 or later.
- A Conductor OVA.

Configure a Conductor

The [Settings](#) page contains many configurable options to help you customize Conductor behavior to support your environment.

When you finish deploying the Conductor in your environment, you may want configure additional settings. See [Best Practices for Conductor Configuration](#) on page 198.

Best Practices for Conductor Configuration

Here are some best practices for configuring your Conductor.

Conductor Initial Setup

Configure these settings when you're setting up your Conductor.

- **Use NTP servers to set System Time** – While you can set your system time manually, using NTP (Network Time Protocol) servers ensures your system time stays synchronized with Coordinated Universal Time (UTC). See [Set the Conductor system time](#) on page 198.
- **Create a human-readable Conductor URL** – You can just keep your Conductor as an IP address, but giving it a human-readable name makes it easier for humans. See [Configure a Conductor IP, Friendly URL, or Port](#) on page 198.
- **Create separate accounts for each person administering the Conductor** - Only use the ‘admin’ account for top-level administration. Creating user accounts for each person who will be administering the Conductor lets you see who is making changes in the system when you review log details. For how to create a user account, see [Add a Person](#) on page 44.
- **Configure email settings** - Configuring your email settings ensures your Conductor has an email address from which to send alerts Airwall and invitations. See [Configure Email Settings](#) on page 200.
- **Get and Set up a CA Certificate** - Setting up a CA Certificate will stop the warnings that your site is unsafe. See [Install a Custom CA Certificate Chain](#) on page 201.

Deploying Airwall Edge Services

- **Add a DNS SRV record pointing to your Conductor** – Adding this record allows easier deployment of physical Airwall Edge Services, as they can find and set the Conductor URL automatically once you connect them to your underlay network. See [Connect an Airwall Gateway with a DNS SRV record](#) on page 247.
- **Configure WiFi Settings** - When you configure WiFi settings on the Conductor, any Airwall Edge Services with WiFi capabilities can retrieve the WiFi settings once they connect to the Conductor. See [Configure WiFi Settings](#) on page 203.

Managing Airwall Edge Services

- **Create Event Monitors** – Create monitors for events to help you manage the activity and health of your Airwall secure network. See [Create an Event Monitor](#) on page 103.

Set the Conductor system time

Set how your Conductor system time is determined.

1. Go to [Settings](#), scroll down to **System Time** and click **Edit Settings**.
2. Under **Use NTP**, click **Enabled**.

 **Note:** You can manually set your system time, but it is a best practice to use an NTP (Network Time Protocol) server.

3. Under **NTP Servers**, enter at least one NTP server, such as *us.pool.ntp.org* or *time.google.com*.
4. Click **Update**.

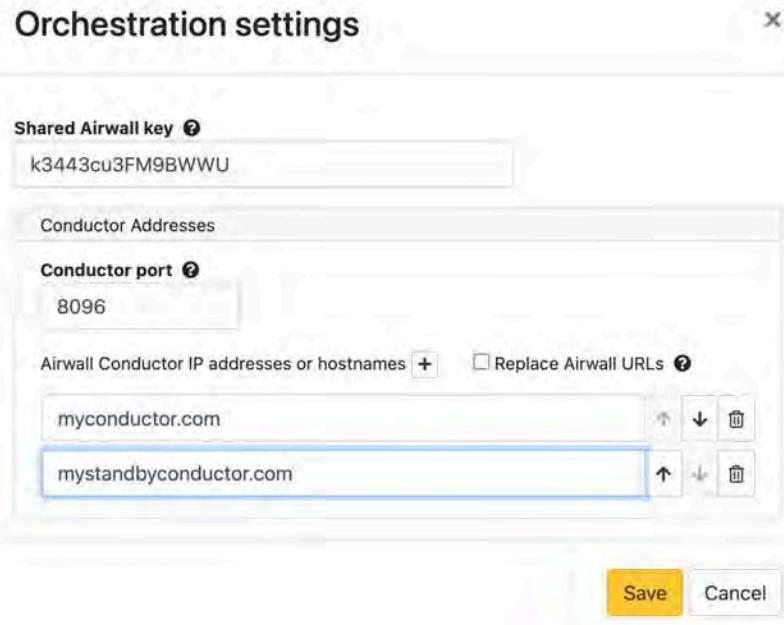
Configure a Conductor IP, Friendly URL, or Port

If you are using a v2.2.10 or later Conductor, you set up the Conductor URL using the [Conductor Configuration Wizard Settings](#) on page 165. Use these instructions to edit the IP, URL, or Port if needed.

v3.0 and later

Friendly URLs cannot have spaces or special characters except - dash.

1. Go to **Settings**.
2. Under **Orchestration Settings**, next to Airwall-Airwall Conductor networking, select **Edit Settings**.
3. The Shared Airwall key is assigned for your Conductor automatically, and you normally do not need to change it.
4. If you need to change the Conductor port, you can do it here.
5. Under **Airwall Conductor IP addresses or hostnames**, select the +, and enter an IP or friendly name for your Conductor.



6. Select **Save**.

You can now use your friendly URL when connecting to the Conductor, and can provide it for others to connect manually, or using Airwall Invitations.

Before v3.0

Friendly URLs cannot have spaces or special characters except - dash.

1. Go to **Settings**.
2. In the **Configuration** section, click **Setup**.
3. Under **Hostname**, enter a friendly name for your Conductor.
4. Under **Domain name**, enter your domain. For example, the settings in the dialog below sets a friendly Conductor URL of friendly.tempered.io:



5. Click **Configure**.

You can now use your friendly URL when connecting to the Conductor, and can provide it for others to connect manually, or using Airwall Invitations.

Configure Email Settings

If you are a member or manager of an Overlay network, you can set up the Conductor to send email notifications when specific events occur there. There are three steps involved: Add your email settings for the Conductor to send email, add emails to receive notifications, and turn on or off notifications.

v3.0 and later

1. Add email settings for the Conductor to set the email address the Conductor sends notifications from.

- a) Go to **Settings > Services > Email Server** and select **Edit Settings**.

If you don't see it as a choice, select **Add service** and select **Email Server**.

- b) Make sure **Enable** is On (green with the bubble to the right).
- c) Enter the settings for the email you want Conductor notifications to come from.
- d) Under **Prefix for subject line**, enter a prefix for the Subject of the emails, if desired. For example, enter **Airwall Alerts**.
- e) Select **Configure**.
- f) Once email settings have been configured, go to **Settings > Services > Email Server** and then select **Send test email...** to verify that the settings are valid.

2. Add emails to receive notifications:

- a) In the Conductor, go to **People**.
- b) Select an existing person, or [Add a Person](#) on page 44.
- c) Under **Alert email trigger level**, select the alert level of notifications for that person to receive.

3. Add the person to the Overlays for which you want them to receive notifications:

- a) Go to **Overlays**, and create or select an Overlay.
- b) On the right, open the **People** tab, and select **Update**.
- c) For the person you want to add to the Overlay, click the column to make them a **Viewer** or **Editor** of the Overlay.
- d) Select **Close**.

Before v3.0

1. Add email settings for the Conductor. This sets the email address the Conductor sends notifications from.

- a) Go to **Settings > Email Server** and click **Edit Settings**.
- b) Click **Enabled**.
- c) Enter the settings for the email you want Conductor notifications to come from.
- d) Under **Prefix for subject line**, enter a prefix for the Subject of the emails, if desired. For example, enter **Airwall Alerts**.
- e) Click **Save**.
- f) Once email settings have been configured, go to **Settings > Email Settings** and click **Send Test Email...** to verify that the settings are valid.

2. Add emails to receive notifications:

- a) In the Conductor, go to **People**.
- b) Select an existing person, or [Add a Person](#) on page 44.
- c) Under **Alert email trigger level**, select the alert level for that person to receive notifications.

3. Add the person to the Overlays that you want them to receive notifications for:

- a) Go to **Overlays**, and create or select an Overlay.
- b) On the right, under **People**, click **Update**.
- c) For the person you want to add to the Overlay, click the column to make them a **Member** or **Manager** of the Overlay.
- d) Click **Close**.

Configure Monitor and Alert Settings

Keep track of the health and activity on your Airwall secure network with monitors and alerts. For more information, see [Monitor Activity with Events and Alerts](#) on page 101.

Install a Custom CA Certificate Chain

You can install or replace a custom CA Certificate chain for the Conductor, which allows the Conductor to generate the CSRs you need to get signed certificates, and so the Conductor can verify the signed certificates you install. When you install custom certificates, they replace the default Tempered factory-installed certificate chain.

Before installing custom certificates on Conductor and Airwall Edge Services, you need to upload the intended certificate chain to Conductor. To install a custom certificate authority chain:

1. Log in to the Conductor with a System Administrator account.
2. Go to **Settings > General Settings > Certificates**.
3. To install certificates initially, select **Install CA certificates**.
To replace certificates, select **Replace CA certificates** (supported in v2.2.8 and later)
4. Select **Choose File** and select a concatenated PEM file containing all of CA chain certificates. This is the certificate chain against which Conductor validates the signed Certificate Signing Request.
5. Select **Upload**.

The Conductor checks that the uploaded certificates validate the chain of trust and are not expired. You can now [Add or Replace a Signed Certificate for the Conductor UI](#) on page 201.

Add or Replace a Signed Certificate for the Conductor UI

Versions	2.2.8Conductors
----------	-----------------

By default, the Conductor comes with a Tempered factory-installed certificate. You can add your own custom certificate to prevent the “Your connection is not private” messages received on some browsers. A custom signed certificate is used by the Conductor for the SSL connection.

Important: For Conductors in HA environments, both Conductors must not be HA paired to upload and install custom certificates. Follow the steps for each Conductor. Once complete, HA pair the Conductors.



Note: When you are in the process of replacing a certificate, the Conductor uses the existing certificate until the replacement is complete.

Before you Begin

Before you can upload or replace a signed certificate, you need to have a CA certificate chain installed so that the Conductor can verify the certificates. For more information, see [Install a Custom CA Certificate Chain](#) on page 201.

Step 1: Request and copy a CSR (Certificate Signing Request) for the Conductor

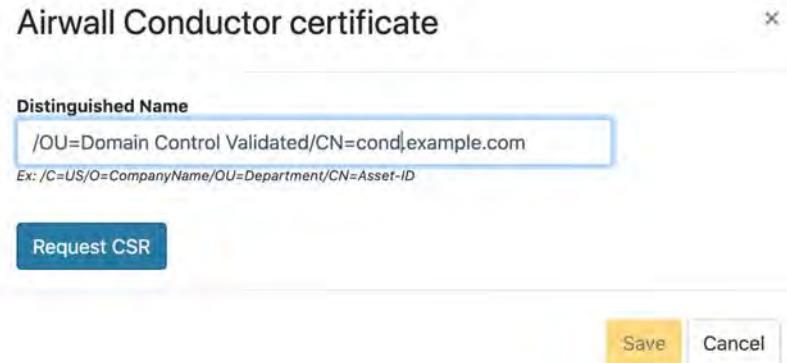
Once you've installed CA certificates (see [Install a Custom CA Certificate Chain](#) on page 201), you can generate a Certificate Signing Request (CSR) to create a certificate (for example, with a PKI Registration Authority):

1. In Conductor **Settings**, under **Airwall Conductor Identity**, click **Actions**, and then select **Create certificate** or **Replace certificate**.

Airwall Conductor identity

Certificate		Actions
Distinguished Name	/OU=Domain Control Validated/CN=kibbles.temperednetworks.com	Create certificate
Status	Active	Replace certificate
Issued by	/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2	Delete
Valid since	01/14/2020	
Valid until	01/14/2021	

- Under **Distinguished Name**, enter the Identity (Distinguished Name) of the Conductor. If you're replacing a certificate, you can leave the Distinguished name the same. For example, /C=US/O=Tempered/OU=Dev/CN=cond.example.com



- Under **CSR**, select either **Copy** or **Download** to generate and get the CSR you need to get a signed certificate. (In versions 2.2.5 and earlier, select and copy the CSR.)
- Select **Save**.

Step 2: Get a signed certificate

Use the CSR to request a new signed certificate. You can generate a new signed certificate using your organization's own process, or with a public PKI Registration Authority.

- Submit the Certificate Signing Request (CSR) you copied or downloaded to your Enterprise PKI Registration Authority. They use it to create your certificates.
- When you get the certificates, download or copy them.

Step 3: Upload the signed certificate to the Conductor

- In Conductor **Settings**, under **General settings**, scroll down to **Airwall Conductor Identity**, and select **Edit**.
- Under **Signed Certificate**, paste the custom-CA signed certificate to install the certificate on the Conductor.



- Select **Save**.
- Refresh your browser window to apply the new certificate.

Configure WiFi Settings

You can configure WiFi settings for connectivity to the underlay in the Conductor. Once a WiFi-enabled Airwall Gateway is assigned to an overlay network, it retrieves the WiFi settings.

Airwall Gateways must first connect to the underlay with a wired connection to retrieve WiFi settings. Once the WiFi settings are configured, the Airwall Gateway will attempt to use those settings whenever the wired underlay connection is unavailable. Simply disconnect the Airwall Gateway underlay wired connection, and it will begin using the WiFi configuration.



Note: You must place the Airwall Gateway into diagnostic mode to configure WiFi settings.



Note: You cannot configure EAP-TLS Wireless networks in conjunction with Customer Certificates.

Set up a WiFi network

The Conductor only supports the configuration of a single WiFi network and this WiFi network is available to all Airwall Edge Services that have WiFi network interfaces. If the WiFi network is deleted, all configured Airwall Edge Services will remove the WiFi network from their configuration.

To configure a WiFi network, go to **Settings > WiFi Networks**, click **New Connection** and enter the wireless network SSID and one of the following authentication options:

- None
- WEP
- WPA-PSK
- EAP-TLS (EAP-TLS is not available on all models)



Note: Prior to defining an EAP-TLS connection, you must have a Customer CA Chain installed on the Conductor. Airwall Edge Services will not apply the EAP-TLS configuration until they have been provisioned with a Customer-signed PKI Certificate. EAP-TLS configurations use the Subject Common Name (CN) component of the Customer-signed Certificate Distinguished Name (DN) as the identity for the EAP-TLS transaction.

The Airwall Gateway automatically detects the wireless family and channel, and has two reverse-polarity SMA (RP-SMA) connectors for antenna connections used in diversity mode to improve wireless signal reception. If only a single antenna is used, connect the antenna to the main antenna connector.

Configure Authentication Options

Manage the settings for user login authentication, such as password requirements and lockout time.

To configure user account settings:

1. Log in to the Conductor with a system administrator account.
2. Go to **Settings > Authentication > Settings > Edit Settings**.
3. Configure **User authentication settings**:

- **Default authentication provider** – Select the default authentication displayed when users log in.
- **Login attempts before lockout** – Set the number of unsuccessful login attempts before lockout. Set to 0 to disable.
- **Password expiration** – Set the number of days until password expires (default 180 days). Set to 0 to disable.
- **Lockout time** – Set the amount of time to track unsuccessful login attempts (default 1 hour).
- **API token expiration** – Set the number of days before API tokens expire. Set to 0 to disable.
- **Show "Forgot Your Password?"** – Check to display a **Forgot your Password?** link that allows a user to reset their password (enabled by default).

4. Configure **Password requirements**:

- **Minimum password length** – Enter the required minimum number of characters
- **At least one number** – Check to require at least one number
- **Upper and lowercase characters** – Check to require both upper- and lowercase letters
- **At least one symbol** – Check to require at least one symbol

5. Configure **Session settings**:

- **Conductor session expiration** – Set the number of hours before a Conductor session expires.
- **Conductor session inactivity timeout** – Set the number of minutes before a Conductor session times out due to inactivity.

6. Configure **Global Airwall agent authentication settings**:

- **Require Airwall agent authentication** – Check to require authentication, and select an option:
 - for all agents to require authentication, which may require some people to update their Airwall Agents)
 - for supported agents to allow older agents that don't support authentication to log in.
- **Require Airwall agent authentication for Linux servers** – Check to enforce authentication for Linux servers. Authentication is not required by default.
- **Retain session on service restart** – Check to allow an Airwall Agent to reconnect to a session after it restarts. By default, restarting ends the session.
- **Require owner for Airwall Agent authorization** – If checked, once an owner is set for an Airwall Agent, no other person will be able to log in from that Airwall Agent.
- **Auto-assign Airwall agent owner on login** – If checked, will assign the first person to log in with an Airwall Agent as the owner.
- **Airwall agent authentication provider** – Select Username and password to require Conductor username and password to log in, choose an authentication provider, or choose All authentication providers to allow the user to select how they log in.
- **Session timeout** – Set the number of hours before an Airwall Agent times out. Note that changing the session timeout does not affect current sessions.

7. Click **Save**.



Note: If you have email settings correctly configured in **Settings > Email Settings**, and you have a **Forgot your Password?** link on the Conductor login screen, all users can enter their username and click the link to send a password recovery email to the address associated with that username.

The password recovery email is sent from the address configured in Email settings, so if it is not set up, users will not be able to recover their passwords this way. If the password recovery email does not arrive within 5 minutes, check your spam folder and explicitly allow the address.

For instructions on setting up Conductor Email settings, see [Configure Email Settings](#) on page 200.

Configure user authentication for Airwall Agents and Airwall Servers

You can configure user authentication for Airwall Agents and the Windows Airwall Server by requiring a username or password before they can connect to an Overlay.



Note:

Linux servers don't support any form of user authentication.



Note: For user authentication compatibility and functionality, make sure your Conductor and all Airwall Agents and Airwall Servers are on the latest version (v3.0).

- In the Conductor, on an Airwall Agent or Server configuration page, select **Edit Settings**, and check the **Require Authenticated Airwall Session**. Select **Update Settings**.

Airwall agent authentication

Require authenticated Airwall session

Provider: Global default (All authentication providers)

Session timeout: Global default (3) hours

Retain session on service restart: Global default (On)



Note: If you don't see the **Edit Settings**, you don't have permissions to edit that Airwall Agent or Server.

- Connect the Airwall Agent or Airwall Server to the Conductor.
- Verify that:
 - Logging in requires you enter Conductor or LDAP credentials.
 - The Airwall Agent or Airwall Server has access to the Overlay.
- You can monitor user connections from the information pages in the **People** tab in Conductor.

You also have the ability to end the session on-demand as an administrator.

Remote Access

End Remote Access Session

(Logged into Windows 7 Client at 05/31/2018 2:14 am from "Windows7VBOX")

See also:

- [Integrate Third-party Authentication with OpenID Connect on page 208](#)
- [Configure LDAP authentication on Conductor and Airwall Edge Services on page 219](#)
- [Walkthrough - Onboard people to your Airwall secure network with User Authentication on page 71](#)

Walkthrough - Onboard people to your Airwall secure network with User Authentication

How to set up global user/password authentication for Airwall Agents and Servers connecting to your Airwall secure network.

This walkthrough walks you through setting up authentication for all people connecting to your Airwall secure network.



Note: This walkthrough covers globally onboarding people with authentication. You can also turn on authentication for individual Airwall Agents and Servers.

Supported Versions

Conductor v2.2.10 and later. This walkthrough is based on v3.0, so some things may be slightly different on earlier versions.

The basic steps are:

- Require User authentication globally.
- Onboard people using People Groups.
- Add people as Remote Access Users.

These steps are covered in more detail below.



Note: For pre-2.2.8 Airwall Agents and Servers only: There is an extra step to provide access at the end of this walkthrough.

Best Practice:

Finding the right balance between ease of use and security is an ongoing challenge.

This walkthrough shows how you can easily onboard and provide trust to a person, but you may choose to keep additional security checks in place, like granting the provisioning request based on the Device ID a person gives you.

A balanced option might include automatic onboarding, but only granting trust to a benign device that they can ping for communication verification and then provide final trust to secure environments once information has been verified verbally.

Step 1: Require user authentication globally

1. Go to **SettingsAuthentication**, and under **Settings**, select **Edit Settings** (in pre-v3.0, this is under **Global Airwall agent authentication settings**).
2. Check or set your authentication options:
 - Check **Require Airwall agent authentication** and select the option for all agents.
 - Under **Airwall agent authentication**, under **Airwall Agent Authentication Provider**, select **Username and password**, or an OpenID Connect (OIDC) third-party authentication provider, if you've set it up. See [auth openid connect.ditamap](#).
 - (Optional) You can also set a custom Session timeout or whether people need to log in when they restart their Airwall Agent

The screenshot shows the "Global Airwall agent authentication settings" dialog box. It includes the following sections:

- Require Airwall agent authentication:** A dropdown menu set to "for all agents". Other options include "Require Airwall agent authentication for Windows servers" and "Require Airwall agent authentication for Linux servers".
- Retain session on service restart:** A checked checkbox.
- Require owner for Airwall agent authentication:** A checked checkbox.
- Auto-assign Airwall agent owner on login:** A checked checkbox.
- Airwall agent authentication provider:** Set to "Username and password".
- Session timeout:** Set to "24 hours".
- Warning message:** "⚠️ Updating the session timeout will not impact any existing sessions".
- Note:** "Settings with an asterisk (*) can be overridden on individual Airwall agents".
- Buttons:** "Save" and "Cancel".

The screenshot shows the same "Global Airwall agent authentication settings" dialog box, but with different checkbox selections:

- Require Airwall agent authentication:** Checked.
- Require Airwall agent authentication for Linux servers:** Unchecked.
- Retain session on service restart:** Unchecked.
- Airwall agent authentication provider:** Set to "Username and password".
- Session timeout:** Set to "24 hours".
- Warning message:** "⚠️ Updating the session timeout will not impact any existing sessions".
- Buttons:** "Save" and "Cancel".

For more information, see [Configure Authentication Options](#) on page 203. You can also require authentication per device on the Airwall Agent or Server page.

Step 2: Onboard People using People Groups

You may also want to [Import people using a CSV file](#) on page 51.

1. Set up a **People Group** on page 74, configuring the onboarding options you want to this People group to have. You can add people on the **People** tab, or add them to the group as you create users in the Conductor.
2. On the **User onboarding** tab:
 - Check **Provide an activation code for each member**.
 - Check **Send onboarding email to users** if you want to send emails automatically.
 - Pre-configure the **General**, **Airwall**, and **Groups** settings for users when they onboard. Setting these options allows members of the group to activate their connections. For more information, see [Connect People's Devices with Activation Codes](#) on page 63.

 **Note:** If you want to configure which version of the Airwall Agent they download, you can set that on the Conductor **Settings** page under **Global Airwall agent settings**.

On the People Groups page, you'll see your new group, and to the right, you'll see the Activation Code icon  that indicates every person added to this group will receive an Activation Code. For more information, see [Connect People's Devices with Airwall Invitations](#) on page 54 or [Connect People's Devices with Activation Codes](#) on page 63.

Step 3: Add Remote Access Users

1. Add the people you want to connect to the Conductor. For Remote Access Users, see [Connect People as Remote Access Users](#) on page 61.
2. As you save each user, from each person's **People** page, add users to the people onboarding group created in Step 2.
 - a) Under **People groups**, select **Edit**.

People groups		Edit...
People group	Activation code	
mobile	None	

- b) Select the onboarding People group created in Step 2.
 3. The people are sent an onboarding email. If desired, you can send them custom instructions, or point them to one of these help topics: [I have a "Finish Setting up my account" email](#) on page 14 or [I have an Activation Code](#) on page 14.
- As people click the link in the email to set their password and log in to the Conductor, they'll be directed to the [Connect an Airwall Agent](#) page where they can install an Airwall Agent or Server and activate their connections.

What's Next

You can get a report on remote sessions from **Visibility > Reports**. For more information, see [Run Network Activity Reports](#) on page 101.

You can see who's remotely logged into your Airwall secure network. See [Check Remote Sessions](#) on page 65.

You can also see which users have used their Activation codes. See [Check Status of People Onboarding](#) on page 64.

For pre-2.2.8 Airwall Agents and Servers only) Give the People group access

If you are onboarding people using pre-2.2.8 Airwall Agents and Servers you need to give the People group access by adding them to Overlays and Relay Rules.

On the Overlay these people need to access, add the People group you created as a **Viewer** (or pre v3.0, as a **Member**).

Select people or groups to view or edit your network

remo

Viewer Editor

cond_remote_users

Remote Access Users

Items 1-2 of 2

Close

Integrate Third-party Authentication with OpenID Connect

You can integrate a third-party authentication provider with person authentication in the Conductor using OpenID Connect (OIDC). If your users are already configured for single sign-on (SSO) with a third party, or if you have a large number of users, this integration streamlines your user management.



Note: You can only configure one OpenID Connect provider on the Conductor at a time. If you need to support many OIDC authentication providers simultaneously, you can choose providers that support federated login so you can connect to one provider and have that provider connect to other providers to authenticate users.



Important: To use OpenID Connect on macOS or iOS Airwall Agents, you must have a public certificate on your Conductor.

User Roles

In the Airwall Conductor, you configure person roles in OIDC by including them in groups. The OIDC group names are pre-configured in the Conductor, so when you make a person a member of one of the OIDC groups in the OIDC provider, they are automatically given that role in the Conductor. For instance, you can declare that all members of the OIDC provider's `cond_system_admins` group are system administrators in the Conductor, and that members of the OIDC `cond_remote_users` group are remote-access users.

Multi-factor Authentication

If your OIDC provider supports a multi-factor authentication (MFA) protocols, you can use MFA on your provider to require MFA for logging into your Conductor or for Airwall Agent session authentication.

Integrate Authentication with the Conductor

To successfully integrate authentication, you must

1. [Create and configure an application in your authentication provider.](#)
2. [Configure OIDC on the Conductor.](#)
3. [Set up Airwall Agents.](#)
4. [Verify third-party authentication is working](#) on page 218

Since each provider is different, refer to the basics required here, and then the [Provider-specific instructions](#) that follow for integrating with some popular providers that support OIDC.

1. *Create and configure an application in your authentication provider*

Create and configure the application in your provider using the [Provider-specific Instructions](#) on page 210 before connecting it to the Airwall Conductor. Each provider's workflow is different, but here are the general steps:

1. Create an OpenID Connect application.
2. Configure it with the following information:

Field	Enter
Name	Whatever you want. For example, “Airwall Conductor”
Login Redirect URI	Your Conductor URI followed by /user/auth/openid_connect/callback. For example: https://conductor.mycompany.com/user/auth/openid_connect/callback. Note – If your Conductor is HA paired, add a second login redirect URI, with the same path added.
Logout Redirect URI	Your Conductor URI: https://conductor.mycompany.com

3. Depending on your provider, set the authentication method to **basic**, or indicate you are using an **authorization code** for authentication (not a refresh token).
4. Allow the **groups** claim for grant. The **groups** claim is what allows the Conductor to match a user’s group with what role they are given. Because **groups** is not a default OIDC claim, it must be turned on in the provider. For more details, see the [Provider-specific instructions](#).
5. Create four groups: cond_system_admins, cond_READONLY_admins, cond_NETWORK_admins, and cond_REMOTE_users to indicate the four different Conductor roles.
6. Add users to each group so they are assigned the correct role when logging into Conductor.
7. Give your users access to the application you created in your provider.
8. If you want to require MFA to log in, set it up in the OIDC provider. Generally MFA is associated with the app. Please consult your provider documentation for detailed instructions on setting up MFA.

2. *Configure OIDC on the Airwall Conductor*

1. Go to Conductor Settings.
2. Next to **Authentication**, select **Add provider**.
3. Select **OpenID Connect** and then select **Next**.
4. On the **Add Authentication Provider** page, under **General settings**, configure the Provider settings as follows (see the [Provider-specific Instructions](#) for help in finding this information):

For this Setting	Enter
Provider Name	Give your provider a descriptive name. This name appears as an option when logging into the Conductor.
Conductor host	Host of your Conductor. Must be in the format https://conductor.mycompany.com (no trailing slash)
OpenID Connect host	Must be in the format https://hostname.com:{optional port}
Issuer	Issuer provided by your OIDC provider. Sometimes this value is the same as the OpenID Connect host depending on the provider.
Client ID (sometimes called Identifier)	Token provided by your OIDC provider associated with the provider application
Secret	Secret token that goes with the Client ID

5. For **HA-paired Conductor host**, enter the Host of your HA Conductor (if applicable).
6. Configure the **Group** settings as follows, and then click **Next**:

For this Setting	Enter
Use groups to manage roles	Checked
System admin groups	Comma-separated list of groups from your provider that will give your user this role.
Read-only admin groups	Comma-separated list of groups from your provider that will give your user this role.
Network admin groups	Comma-separated list of groups from your provider that will give your user this role.
Remote-access user groups	Comma-separated list of groups from your provider that will give your user this role.



Note: If users are in groups that match more than one of the roles, they are given the highest level of access possible (system admin, read-only admin, network admin, then remote-access user).

7. Configure any Group filters you want, and click **Finish**.
8. If you have non-public DNS servers configured in the Conductor under **Global Airwall Agent/client settings**, your users won't be able to reach the public addresses on their devices that include the OpenID Connect providers. You may need to configure DNS servers on the Conductor to add your OpenID Connect provider's DNS server.
9. After changing OIDC configuration, you need to log out and log back in to the Conductor to restart it. When you log back in, you can now choose your third-party authentication provider.

3. Set up the Airwall Agents

Any Airwall Agents authenticating using your third-party provider also need to be set up:

1. [Provision and License Airwall Edge Services](#) on page 161 in the Conductor.
2. Go to the **Overlays** page, scroll down to **People**, and click **Update**, and add the Airwall Agent as a member.
3. Also check that:
 - a) Airwall Agents are included in your Airwall Relay rules.
 - b) Airwall Agent devices have been added to the appropriate Overlays, and you've set device trust on the Overlays as needed.

Your users should now be able to log in using the third-party authentication provider.

Require third-party authentication

You can also require users to authenticate using the third-party provider either individually or as a group (in 2.2.3 and later Conductors). On the agent's **Airwall Agent** tab, or on a **People Group Properties** tab:

- Check the **Require Authenticated Airwall Session** box.
- Under **Provider**, choose the third-party authentication provider you created.

Provider-specific Instructions

Here are specific instructions for a few of the common third-party authentication providers. Note your provider's documentation may be more up-to-date.

Okta - Create Application and Set Up Group Claims

Create an Application

1. In Okta, go to **Applications**.
2. Select **Add Application**.
3. Under **Create New Application**, select **Web**.
4. Set **Allowed grant type** to **Authorization code**.

5. Set the **OpenID Connect host** to the same value as the **Issuer** in Conductor. This value is found on the under **OpenID Connect ID Token** on the **Sign on** tab.
6. Note the Client ID and Secret that are in your application, on the **General** tab under **Client Credentials**.
7. Set up Groups Claim (see below).

Set up Groups Claim

To set up Okta to allow the groups claim in OpenID Connect, use the Classic UI.

1. In Okta Authentication, go to **Security**, and select **API**.
2. From the **Authorization Servers** tab, open the default API (or whatever API you are assigning to your application).
3. On the **Scopes** tab:
 - a) Add a scope named `groups`.
 - b) Uncheck **Set as Default**.
 - c) Check **Include in Public Metadata**.
4. On the **Claims** tab:
 - a) Add a claim named `groups`.
 - b) Set **Include in token type** to **ID Token / Always**
 - c) Set **Value type** to **Groups**
 - d) Set a filter of **Matches regex** to `.*`. Alternatively, set a filter of **Starts with** and set to the prefix for your group names that you want to use in Conductor. For example, set **Starts with** to `cond_`.
 - e) Set **Include in** to **Any scope**.

OneLogin - Create Application

1. In OneLogin, select **Add App**, and then choose **OpenID Connect (OIDC)**.
2. Set **Authentication method** to **basic**.
3. Add users to the roles you want. For example, to make them a system admin, add them to `cond_sysadmins`.

 **Note:** In OneLogin, roles are mapped to OIDC groups (groups mean something else), so add users to roles, not groups.
4. In your OneLogin application, on the **Parameters** tab, configure the roles-to-groups mapping. Edit the groups and modify the default on the **Roles** field to: **User roles, --No transform--**.
5. Note the information you'll need to configure the Conductor:
 - a) **OpenID Connect host**: This is your OneLogin login URL, for example, `https://my-company.onelogin.com`.
 - b) **Issuer**: On the **SSO** tab, select **OpenID Provider Configuration Information** for the **Issuer**.
 - c) **Client ID and Secret**: These are both on the **SSO** tab.

Auth0 - Create Application

1. In Auth0, under **Applications**, select **Create Application**, and then **Regular Web Application**.
2. Skip the quick start.

3. On your new application's **Settings** page:
 - a) Change **Application Properties** > **Token Endpoint Authentication Method** to **Basic**.
 - b) In **Application URIs** > **Allowed Callback URLs**, add the login redirect URI. See the Login Redirect URI near the top of this page.
 - c) In **Application URIs** > **Allowed Logout URLs**, add the logout redirect URI. See the Logout Redirect URI near the top of this page.



Note: Auth0 does not currently support OpenID Connect Logout.

- d) Note the following information in Auth0 that you'll need to configure the Conductor:
 - **Basic Information** > **Domain**: On the Conductor, you enter this information as **Open Connect host** and **Issuer** (note that the https is required).
 - **Basic Information** > **Client ID** and **Client Secret**: On the Conductor, you enter this information as Client ID and Secret.
 - e) When finished, select **Save Changes** at the bottom of the **Settings** page.
4. Add the rule required by Auth0 to set OIDC groups. (In Auth0, roles map to groups on the Conductor.)
 - a) Under **Auth Pipeline** > **Rules**, select **Create Rule**.
 - b) Select **Empty Rule**.
 - c) Set the name to **Add groups to OIDC token**.
 - d) Add this rule:

```
function (user, context, callback) {
  const namespace = 'https://<your issuer>';
  const assignedRoles = (context.authorization || {}).roles;

  let idTokenClaims = context.idToken || {};
  let accessTokenClaims = context.accessToken || {};

  idTokenClaims[`$${namespace}/groups`] = assignedRoles;
  accessTokenClaims[`$${namespace}/groups`] = assignedRoles;

  context.idToken = idTokenClaims;
  context.accessToken = accessTokenClaims;

  callback(null, user, context);
}
```

- e) Change the namespace in the rule to be your Auth0 issuer. Example: <https://dev-abc123.auth0.com>
5. Following Auth0 instructions, add roles to users that give them the proper role in the Conductor.

Azure Active Directory - Create Application

Note that the Azure AD documentation may be more up-to-date and the settings in your Azure AD account may vary.

1. In Azure Active Directory (AD), select **App registrations**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the 'Microsoft Azure' logo and a search bar. Below the header, the title 'Default Directory | Azure Active Directory' is displayed. On the left side, there's a navigation sidebar with several sections: 'Overview' (highlighted with a light gray background), 'Getting started', 'Preview hub', and 'Diagnose and solve problems'. Under the 'Manage' heading, there are links for 'Users', 'Groups', 'External Identities', 'Roles and administrators', 'Administrative units', 'Enterprise applications', 'Devices', 'App registrations' (which has a yellow arrow pointing to it), 'Identity Governance', 'Application proxy', 'Licenses', 'Azure AD Connect', and 'Custom domain names'.

2. Select **New Registration**, and fill in the form as follows:

- **Name** – Enter a name for the Application (for example, "Airwall Conductor").
- **Supported account types** – Select **Accounts in any organizational directory (Any Azure AD directory – multitenant)**.
- **Redirect URI** – Select **Web**, and then enter the URL of your Conductor followed by /user/auth/openid_connect/callback:

The screenshot shows the 'Register an application' form in the Microsoft Azure portal. The 'Name' field is filled with 'Airwall Conductor'. The 'Supported account types' section has the 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)' option selected. The 'Redirect URI (optional)' field contains 'https://airwall-rs.tempered.io/user/auth/openid_connect/callback'. A note at the bottom states: 'By proceeding, you agree to the Microsoft Platform Policies'.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Default Directory >

Register an application

* Name
The user-facing display name for this application (this can be changed later).
Airwall Conductor

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Default Directory only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only
Help me choose...

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web https://airwall-rs.tempered.io/user/auth/openid_connect/callback

By proceeding, you agree to the Microsoft Platform Policies

Register

3. Click **Register**. Take a note of the Application (client) ID and the Directory (tenant) ID provided by Azure AD.

Once you've registered the Application, Azure AD provides a set of IDs that you configure in the Conductor when you set up Azure AD as an OIDC provider. Here is how they map to the Edit Authentication Provider options in the Conductor:

The screenshot shows the 'Edit Authentication Provider' page in the Airwall Conductor interface. On the left, there's a sidebar with 'Overview', 'Quickstart', 'Integration assistant', 'Manage' (selected), 'Branding', and 'Authentication'. The main area has tabs for 'Essentials', 'General settings', and 'Provider name (optional)'. Under 'General settings', there are fields for 'Conductor host' (https://), 'OpenID Connect host' (https://sts.windows.net), 'Issuer' (https://sts.windows.net/8040...), 'Client ID' (0dfa8445-5500-4ee8-9cf2-f894...), and 'Secret' (a masked password). Yellow arrows point from the 'Application (client) ID' and 'Directory (tenant) ID' fields in the sidebar to the 'Client ID' and 'Issuer' fields respectively. Another yellow arrow points from the 'Object ID' field to the 'Client ID' field.

- Application (client) ID – Enter in the **Client ID** box.
- Directory (tenant) ID – Append this ID to <https://sts.windows.net/> and enter in the **Issuer** box .

4. In Azure AD, create a Client Secret:

- a) Select **Certificates & secrets**.
- b) Select **New client secret**.

Airwall Conductor | Certificates & secrets

Certificates
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID
No client secrets have been created for this application.			

- c) Add a description, and select when the secret expires.

Add a client secret

Description

Expires
 In 1 year
 In 2 years
 Never

Add **Cancel**

- d) Select **Add**.

5. On the **Client secrets** page, copy the **Value** (not the ID). Enter the Value as the secret in the Conductor.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID
Conductor Client Secret	12/31/2299	1RXRab-JVzKowS2ZI4I9_p_1bm-k-3	eb780cff-a4ed-44d5-8a-97bae7f51bf7

Edit Authentication Provider

General settings

Provider and audience	Conductor host
Azure AD	https://

In your OpenID Connect provider, set the login redirect URL to https://airwall.conductorairwall.com/login/auth/oidc/redirect/IAuth. Set the logout redirect URL to https://airwall.conductorairwall.com/logout.

OpenID Connect host
https://sts.windows.net/
Issuer
https://sts.windows.net/B0D40...

Client ID
B0f84...
Secret

Use OpenID Connect logout

6. From the newly registered application in Azure AD, select **Authentication**.

7. Under **Implicit grant**, verify that **Access tokens** is checked.

The screenshot shows the Azure portal's 'Authentication' configuration page for the 'Airwall Conductor' application. On the left sidebar, 'Implicit grant' is selected under the 'Authentications' section. In the main pane, the 'Implicit grant' section is expanded, showing the following configuration:

- Redirect URIs:** https://airwall-conductor.azurewebsites.net/callback
- Logout URL:** https://airwall-conductor.azurewebsites.net
- Implicit grant:** A note states: "Allow an application to request an access token from the authorization provider. Including Access tokens and ID tokens is recommended only if the application has a single usage architecture. APIs that interact with component, please use the authentication of OAuth 2.0 with code flow, or it includes a multi-Auth mechanism. An OAuth 2.0 endpoint is required." Below this, there are two checkboxes: 'Access tokens' (which is checked) and 'ID tokens'.

8. In the Azure AD application, set up the groups claim:
- From the menu on the left, select **Token configuration**.
 - Select Add groups claim.
 - Check all of the group types:

The screenshot shows the 'Edit groups claim' configuration page. The 'Supported account types' section is expanded, showing the 'All groups' checkbox selected. Below this, the 'Customize token properties by type' section is expanded, showing three dropdown menus: 'ID', 'Access', and 'SAML'.

- Under Customize token properties by type, expand and configure the properties as follows:
 - ID** – Select **sAMAccountName**.
 - Access** – Select **sAMAccountName**.
 - SAML** – This is not used.

9. In Azure AD, create the groups you want to use for the Conductor. Here are some suggested groups:

- cond_network_admins
- cond_READONLY_admins
- cond_REMOTE_users
- cond_SYSTEM_admins

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure' and a search bar. Below it, the breadcrumb navigation shows 'Home > Default Directory > Groups | All groups'. On the left, there's a sidebar with 'All groups', 'Deleted groups', 'Diagnose and solve problems', 'Settings' (with options for General, Expiration, Naming policy), 'Activity', 'Privileged access groups (Preview)', and 'Access reviews'. The main content area displays a table titled 'Groups | All groups' with columns for 'Name', 'Object Id', and 'Group type'. Four groups are listed:

Name	Object Id	Group type
cond_network_admins	414ec0b1-e7f4-4499-a830-98d...	Security
cond_READONLY_admins	d3921313-00d1-4391-8196-7...	Security
cond_REMOTE_users	cd12a46e-0d93-458c-b126-68...	Security
cond_SYSTEM_admins	7777f1de-6c61-42a0-813d-6a...	Security

10. Add users to Azure AD, and assign them to the appropriate groups for Conductor access:

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure' and a search bar. Below it, the breadcrumb navigation shows 'Home > Default Directory > Users > Network Admin'. The main content area displays a user profile for 'Network Admin' (netadmin@onmicrosoft.com). The profile includes a large orange circular icon with 'NA' in white. The 'Manage' sidebar on the left lists 'Profile', 'Assigned roles', 'Administrative units', 'Groups', 'Applications', 'Licenses', and 'Devices'. The user details show 'User signed in' and 'Group memberships' (1). A yellow arrow points to the 'Group memberships' link.

You are now ready to configure Azure AD as an OIDC provider in the Conductor as described in [2. Configure OIDC on the Airwall Conductor](#) on page 209. For the mappings from Azure AD to the Conductor, see steps 3 to 7 above.
Verify third-party authentication is working

To verify your configuration:

1. Log out of Conductor.
2. Open an incognito window and log in, choosing the provider name you chose in the Conductor.
3. Log in as a user you've set up with third-party provider. You should be able to log in to the Conductor using your third-party provider credentials.

To verify a client can connect:

- After the client logs in using the third-party provider, ping the client.

Troubleshooting Third-party Authentication User Login

If user login is failing with “Could not find that username/password combination,” verify:

- The user has been given access to your OIDC application in the third-party provider
- The user is a member of a group in your provider that is mapped to a user role in the Conductor
- The “groups” claim is allowed in your application in the provider
- The user typed in their username and password correctly

Check the Conductor log for additional clues for why the login failed. For instance, you may see a log message that a person does not match any groups to get a role.

Configure LDAP authentication on Conductor and Airwall Edge Services

You can use Active Directory and LDAP authentication with the Conductor to streamline user account management. When LDAP is configured, users can choose to log in with an LDAP account on the Conductor login page.

There are currently three different ways to authenticate with Conductor.

- With a Conductor account. These are local accounts that log directly into the device
- With LDAP authentication. This allows you to authenticate with any LDAP server, including Microsoft Active Directory services.
- With a third-party authentication provider that supports OpenID Connect. See [Integrate Third-party Authentication with OpenID Connect](#) on page 208.

To set up a LDAP authentication, you need to already have an LDAP server accessible to the Conductor.



Note: These instructions use Microsoft Active Directory, but other LDAP services also work.

There are four different roles in the Conductor:

- **System Administrator** – These users have full access to the Conductor and can adjust any settings. Note that to edit LDAP settings, you must be logged in locally to the Conductor, not through LDAP.
- **Read-only System Administrator** – These users have read access to the Conductor, but cannot make changes.
- **Network Administrator** – These users have access to and can adjust any overlay network they are a manager of. They do not have access to Conductor Settings.
- **Remote Access User** – These users can only see their own information, and can log in with their credentials if authentication is required for their Airwall Agent or Server.

For more detailed role information, see [Understand People Roles and Permissions](#) on page 49.

Step 1: Set up and configure your LDAP server

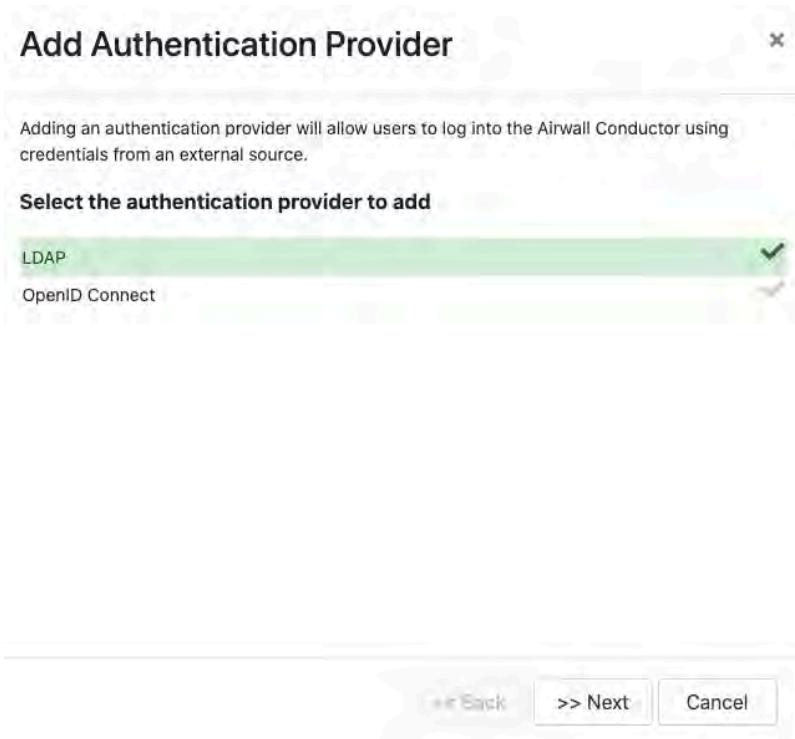
LDAP is not enabled in Active Directory by default, so you will have to turn it on. Once you have LDAP working and running, you can start.

Create a dedicated account with the necessary permissions to authenticate. In Active Directory, you could create a service account under the root "Users" OU, and make it a Domain Admin.

Step 2: Enter and verify your local Conductor admin account credentials, and select Authentication provider

1. Log into Conductor locally (not through LDAP) as a System Administrator. (Only local administrators have access to authentication provider settings.)
2. Open **Settings**, and next to **Authentication**, select **Add Provider**.

3. Select **LDAP** from the list of providers.



Step 3: Enter your LDAP settings

You will need to know the following values:

- Host (Hostname or IP address)
- Port (636 is the default)
- If you are using a dedicated LDAP service account, the fully-distinguished path for the user account, and the password

Under **LDAP host settings**, enter the information for your LDAP host, and select **Next**. For more details on these settings, see [LDAP host settings](#) on page 225.

Edit Authentication Provider

LDAP host settings

Host	Port
192.168.88.10	636
Bind DN <small>(leave blank for anonymous access)</small>	Password
cn=conductor LDAP, cn=users, dc=ldap.	*****
Connect method	SSL

Validate server certificate

Test connection

[<< Back](#) [>> Next](#) [Cancel](#)



Note: TLS LDAPS communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged.

Step 4: Configure Search Settings

This page can mostly be left as-is, unless you have special settings you wish to set. You can search for user accounts here to ensure that the Conductor can search the directory. Select **Next**. For more details on these settings, see [LDAP search settings](#) on page 226.

Edit Authentication Provider

LDAP search settings

Base search DN	User UID attribute
dc=serverpod,dc=net	sAMAccountName
Custom search filter	<small>Eg. (department=IT), (objectClass=person), etc</small>
(memberOf=CN=Developers@TempNetworks,OU=TempNetworks,OU=Host)	

Test LDAP search

tnw **Test LDAP search**

1 Enter a user name and click the 'Test search' button to test searching for a user

[<< Back](#) [>> Next](#) [Cancel](#)

You can test the search by entering a search term and selecting **Test LDAP search**.

Step 5: Configure Group Settings

The Conductor assigns LDAP users to one of the four account types above by making them a member of a security group.

If you don't have appropriate groups already, create these groups in LDAP to link to Conductor roles (you can use different names – using cond_ makes it easier to see which roles are for the Conductor). By default, these groups place the users into the following roles:

- **cond_admin** – System Administrator
- **cond_READONLY** – Read-only System Administrator
- **cond_NETWORK** – Network Administrator
- **cond_REMOTE** – Remote Access User

Since users cannot have more than one role at a time, if they are members of multiple groups, they'll be assigned the role with the most permissions.

Remember to test the settings to ensure that Conductor can see all of the groups you reference on your LDAP server.

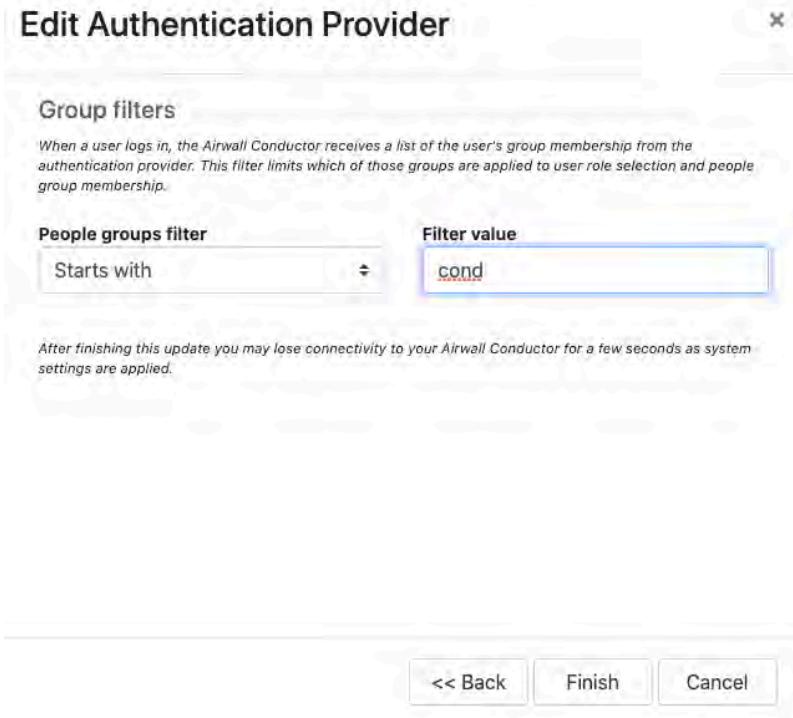
1. For **LDAP group settings**, enter the groups for the roles you want LDAP users to have, and **Group search attributes**, and select **Next**. For more details on these settings, see [LDAP group settings](#) on page 227.

The screenshot shows the 'Edit Authentication Provider' dialog box with the 'LDAP group settings' tab selected. The 'Enabled' button is highlighted. The 'System admin groups' section contains 'cond_admin'. The 'Read-only admin groups' section contains 'cond_READONLY'. The 'Network manager groups' section contains 'cond_NETWORK'. The 'Remote-access user groups' section contains 'cond_REMOTE', which is highlighted with a blue border. Below these sections are 'Group search attributes' fields for 'Group class name' (containing 'group') and 'Group attribute name' (containing 'member'). At the bottom left is a yellow 'Test group settings' button. At the bottom right are buttons for '<< Back', '>> Next', and 'Cancel'.

You can also add other security groups to the configuration, separated by commas.

-  **Note:** You can set up these groups on your LDAP server after setting up LDAP on the Conductor, but **Test group settings** will fail.

- For **Group filters**, enter filters to specify which LDAP groups the Conductor sees. For example, if you've created the cond_groups above, you may want to set the filter to **Starts with** with a value of cond.



- Select **Finish**

You may lose connection briefly as the new settings are applied.

Step 6: Configure user onboarding

Configure user onboarding for the people groups created above to give users access to overlay networks through Airwall Agents and Servers. Setting the groups up beforehand simplifies user onboarding.

- In the Conductor, create **People groups** that match the LDAP groups you specified above (for example, cond-admin)
- Specify user onboarding options as you create the groups. For details, see [Set up a People Group](#) on page 74.

As users log in through LDAP, they are added to these **People groups** and given an activation code that activates the permissions and other options you specified for the **People groups**.

Step 7: Set up Conductor management access

You can also set up access for your Conductor system and network admins individually.

- 1. Add administrators to Overlays** – Add administrators individually as members of Overlay networks to give them access to the resources they need. You can add them from their **People** page, or from an Overlay page:

 - From the person's **People** page, next to **Overlay networks**, select **Edit**. Add the person as a member or manager of Overlays.

The screenshot shows the 'People - Local Administrator' page in the Conductor interface. On the right side, there is a section titled 'Overlay networks' with an 'Edit...' button. Above this, under the heading 'Info', it says 'No tags in use'. Below 'Info' is a section titled 'People groups' with an 'Edit...' button, stating 'Not a member of any people groups'. The main area contains various user profile fields: Local Administrator Account, User directory (Local Accounts), Full name (Local Administrator), Username (admin), Role (System Administrator), Status (Active), API access (Disabled), Email (global-admin@temperednetworks.com), Phone, and Alert email trigger level (None). Each field has its current value displayed next to it.

Edit memberships

The screenshot shows the 'Edit memberships' dialog. It has two columns: 'Network' and 'Member'. Under 'Network', there are two entries: 'Remote user network' and 'Contractor network', each with a green checkmark indicating they are selected. At the bottom right of the dialog is a 'Close' button.

- From the **Overlays page**, open the overlay, and under **People**, select **Update**. Add the administrators as members or managers of the overlay.

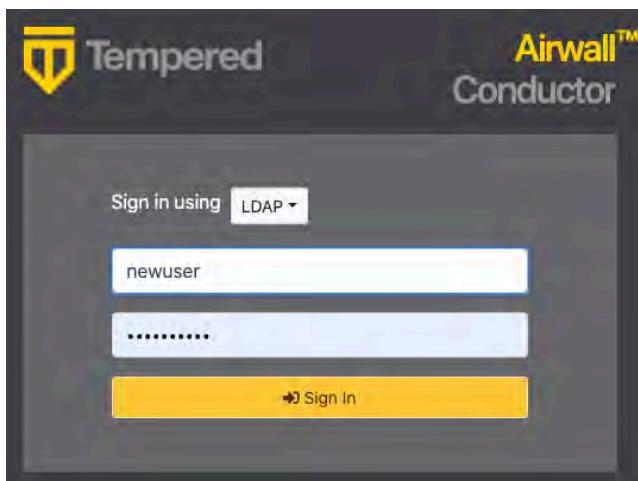
The screenshot shows the 'People' page with an 'Update' button at the top right. Below the button, there are two entries: 'Sys Admin' and 'Manager', each preceded by a small user icon.

2. **Add administrators to People groups** – Similarly, you can add administrators to **People groups**, from their People page or add several administrators from the People group:
 - **From a person's People page** – Next to **People groups**, select **Edit** and select the **People groups** with the permissions they need.
 - **From a People group** – Open the **People group**, and on the **People** tab, select the people to add.

Step 8: Verify by logging in to the Conductor

Verify that LDAP is set up by logging in and checking permissions.

1. Log out from your local administrator account.
2. Next to **Sign in using**, select **LDAP**, and log into the Conductor with an LDAP account.



3. Check that permissions are set correctly for that user.

See also: [Configure user authentication for Airwall Agents and Airwall Servers](#) on page 204.

LDAP host settings

LDAP host setting	Description
Host	The hostname or IP address of your Active Directory or server.
Port	<ul style="list-style-type: none"> • Select 389 for Plain or TLS - This option is only available for SSL or TLS connect methods, and is only enabled if you have uploaded CA certificates. • Select 636 for SSL. <p>Note: TLS LDAPS communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged.</p>

LDAP host setting	Description
Bind DN	<p>If you are using a dedicated LDAP service account, enter the fully-distinguished path for the user account, and then enter the password for the account in the next box.</p> <ul style="list-style-type: none"> • CN=<i>User Full Name</i> • CN=<i>User OU</i> • DC=<i>Domain Component 1</i> • DC=<i>Domain Component 2</i> <p>An example of a fully-distinguished path:</p> <p>CN=ldapServiceAccount, OU=ServiceAccounts, OU=Users, DC=mySecureCorpDomain</p> <p>If you are using user accounts for LDAP Bind connection authentication and authorization, leave Bind DN and Password blank, providing anonymous access.</p>
Password	Enter the password for the user account (specified in BindDN) used to connect to the LDAP service. Leave blank if Bind DN is blank.
Connect method	<ul style="list-style-type: none"> • Plain - Do not use encryption to communicate with the LDAP server. Not recommended. • SSL - Use the SSL protocol to communicate with the LDAP server. • TLS - Use the TLS protocol to communicate with the LDAP server.
Validate server certificate	Select to validate the LDAP server's security certificate against the local CA certificate store.

LDAP search settings

LDAP search setting	Description
Base search DN	Enter the root of the tree in LDAP, underneath which your users and groups are defined.
User UID attribute	<p>Enter the name of the attribute that contains the user's login name:</p> <ul style="list-style-type: none"> • For Active Directory: <i>sAMAccountName</i> • For LDAP: <i>uid</i>
Custom search filter	Use to limit user search results, or to filter to only user entries in LDAP (filtering out non-user entries that are present in the user directory).

LDAP search setting	Description
Test LDAP search	<p>Enter a username and click Test LDAP Search to test your search settings. This test queries the LDAP directory for the given user using your current settings, and displays the number of records located, if any.</p> <p>Best Practice: Make sure this test is successful before continuing.</p>

LDAP group settings

LDAP group setting	Description
System admin groups	Add the LDAP groups that contain members you want to have System Administrator access. Add only trusted groups to this setting.
Read-only admin groups	Add the LDAP groups that contain members you want to have read-only access. Add only trusted groups to this setting.
Network manager groups	Add the LDAP groups for members you want to have permissions to manage overlay networks. You can define which overlay networks they have access to by onboarding people using People groups before they log in, or individually after the user has logged in for the first time.
Remote access user groups	Add the LDAP groups for members you want to have remote access. You can define which overlay networks they have access to by onboarding people using People groups before they log in, or individually after the user has logged in for the first time.
Group class name	<p>Enter the name of an objectClass that the group entry must contain in the LDAP directory, such as:</p> <ul style="list-style-type: none"> • Active Directory: <i>group</i> • LDAP: <i>posixGroup</i>
Group attribute name	<p>Enter the name of the attribute in the group entry that contains the list of users in that group:</p> <ul style="list-style-type: none"> • Active Directory: <i>member</i> • LDAP: <i>memberUID</i>
Test group settings	<p>Select to test your group settings.</p> <p>Best Practice: Make sure this test is successful before continuing.</p>

Configure LDAP to manage user roles

You can use Active Directory and LDAP authentication with the Conductor to streamline user account management. When LDAP is configured, users can choose to log in with an LDAP account on the Conductor login page. See [Configure LDAP authentication on Conductor and Airwall Edge Services](#) on page 219.

1. Log in to the Conductor with a System Administrator account and go to **Settings > Authentication > External authentication providers**.
2. Next to **LDAP**, and click **Next**.
3. Enter the LDAP host settings (see [LDAP host settings](#) on page 225), and click **Test Connection** to validate that the your LDAP settings are valid, then click **Next**.

4. Enter the LDAP search settings (see [LDAP search settings](#) on page 226) and click **Test LDAP search** to validate that your LDAP search is valid. Once the test confirms a valid LDAP search, click **Next**.
5. Determine whether you want to use LDAP groups to manage Conductor user roles:
 - To use LDAP groups: Enter the LDAP group settings (see [LDAP group settings](#) on page 227), and click **Test** to verify the group settings. Once the test confirms your group settings, click **Finish**.
 - No LDAP groups: If you do not want to use LDAP groups, simply click **Finish**.

Your LDAP configuration is now complete, and can be managed as needed in **Settings > Authentication**.



Note: TLS LDAPS communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged.

Optional Conductor Configuration

How to configure optional features on your Conductor.

Configure a Conductor for High Availability

Conductor High Availability (HA) provides hardware redundancy between two Conductors and requires a manual failover. When creating a Conductor HA pair, one Conductor is assigned as the active and the second is assigned as the standby. The active Conductor is used to manage Airwall Edge Services, overlay networks and communications policies.

As a system administrator, you can access a standby Conductor, but only limited functionality is available. In standby mode, the Conductor is kept in sync with the active Conductor, but has limited functionality as follows:

- Read-only database
- Conductor HA configuration changes
- System setup changes
- Firmware updates

Using failover

You need to manually initiate failover between the active and the standby Conductor. The manual failover can take several minutes to complete. During this time, the Airwall Edge Services and devices continue to operate in their current configurations, and overlay network communications are not interrupted.

Automatically Create an Standby HA Conductor in the Cloud

The Conductor has automated the process of setting up a High Availability (HA) Conductor in the cloud.

Once you've set up the cloud provider on your active/master Conductor, setting up and configuring a standby using the Conductor is simple and eliminates many of the mistakes that can happen when manually configuring a standby Conductor in the cloud.

Before you begin

Before you can create a cloud standby Conductor automatically, you must:

- Have an account with a cloud provider
- Have your active/master Conductor set up in the same cloud provider
- Have a Conductor voucher for your new standby Conductor
- Set up a cloud provider in the Conductor. See [Set up Cloud Providers](#) on page 364.

To set up a Cloud HA Conductor

1. On the Conductor that you want to be active for the HA pair, go to the **Settings** page.
2. On the **Cloud providers** tab, select **Create cloud**.

- Under **Conductor HA**, select the same cloud provider as your active Conductor.

Configured cloud providers

Cloud Provider	Route Injection	Default Region
Alibaba Cloud	Disabled	us-east-1
Alibaba Cloud route injection	Disabled	us-east-1
Default region		
AWS route injection	Disabled	eu-central-1
Default region		

Airwall templates: None specified

- On the **Create cloud** page:
 - Name** – Enter a deployment name for your standby Conductor.
 - Conductor Voucher** – Add the Conductor voucher for your standby Conductor.
 - Default region** – Select your region from the cloud provider list.
- Under **Image and network options**, select the cloud provider details for your new Conductor. Only Conductor images matching your active Conductor are displayed. Select the **Network (VPC)** to bring up the options for the public subnet from your cloud provider.

Create cloud

Name: test-sb-sung **Conductor Voucher**: BA9B172FA2A9EC18

Default region: eu-central-1

Image and network options

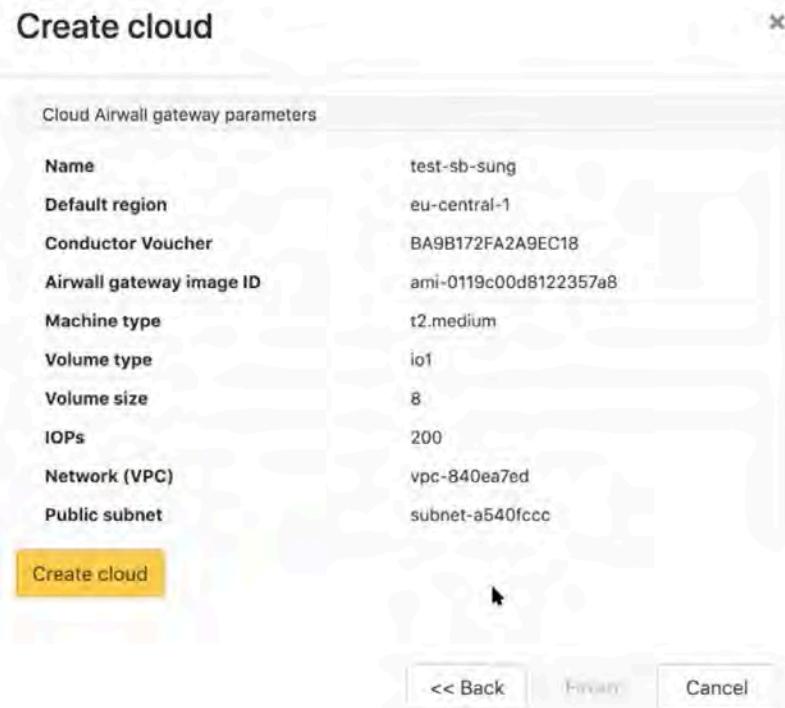
Airwall gateway image ID : Conductor-401v-hvm-r2.2.8-1244	Machine type : T2 Medium Instance
Volume type : io1	Volume size : 8
Network (VPC) : default-vpc	IOPS : 200

Public subnet: Public (subnet-a540fccc) | eu-cen

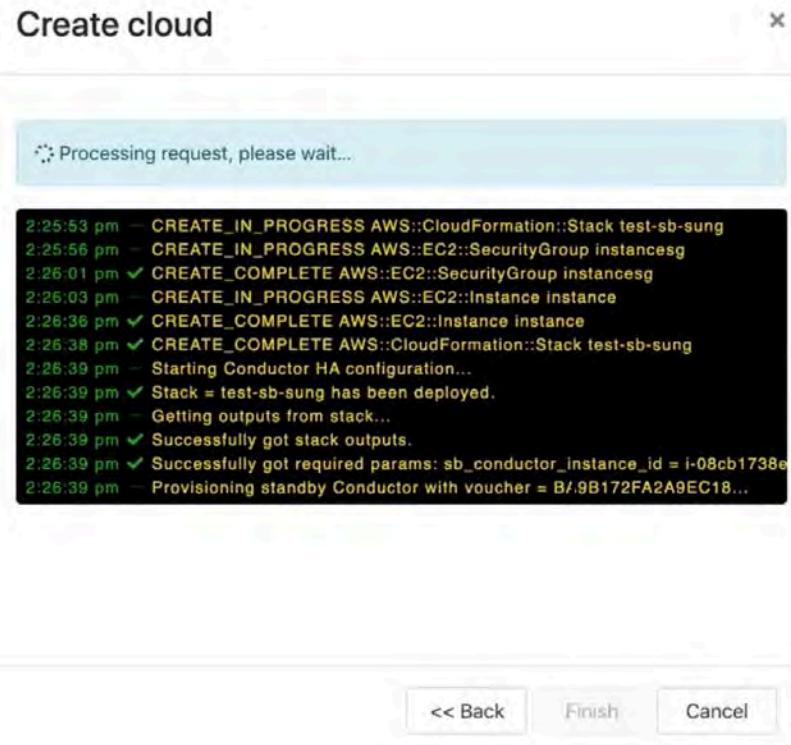
<< Back >> Next Cancel

- Click **Next**

7. Check that the parameters are correct, and click **Create cloud**.



8. Wait for the active Conductor to create and provision a new Conductor, and then configure it automatically as a standby Conductor. The **Create cloud** HA Standby process adds port 5432 to the existing security group of the active Conductor (or creates it if it doesn't have one), and then sets Conductor HA settings to both active and standby Conductors with the information from your current active Conductor. Depending on your cloud provider, this process can take up to 10 minutes.



9. When it is done, select **Finish**.

10. As part of the provisioning process, you are logged out and will see a **Not connected to the Airwall Conductor** message. When this happens, log back into the active Conductor.
11. On the **Dashboard**, under **Recent Events**, you'll be able to see the HA Standby Conductor was created.

The screenshot shows the Conductor dashboard with the following details:

- System stats:**
 - Total Airwalls: 0
 - Airwall gateways online: 0 (Out of 0)
 - Airwall agents online: 0 (Out of 0)
 - Airwalls that can be upgraded: 0
 - Total devices: 0
 - Authenticated Airwall sessions: 0
 - Recent logins: 1
- Navigation:** System, Airwalls, Overlays, Devices.
- Messages:** Welcome to the Conductor! Enjoy your stay. Posted by System at 03/27/2020 4:26:52 pm.
- Recent events:** Conductor HA-pair Created standby HA pair View

Your standby HA Conductor is set up, provisioned, and configured.

Check the Status of your Standby Conductor

1. On your active Conductor, go to the **Settings** page.
2. Under **Airwall Conductor high availability**, you can see the status. It may say **Not streaming** until the cloud HA standby Conductor is fully set up on your cloud provider.

The screenshot shows the "Airwall Conductor high availability" section of the Settings page. It displays the following information:

HA configuration		
HA peer device ID	HA peer replication IP	Replication status
AMA@40130#EC2BB8146BB3	18.197.106.15	Streaming

Edit settings

Once it says **Streaming**, your standby Conductor is ready and acting as a standby HA Conductor. You can also check on your cloud provider to see the new standby Conductor instance.

Log in to your Standby Conductor

Once your standby Conductor shows as **Streaming** on your active Conductor's **Settings** page, you can log in to the standby Conductor.

1. In your active Conductor, go to **Settings** and scroll down to **Airwall Conductor high availability**.
2. Copy the **HA peer replication IP** and enter it into a web browser.
3. Log in with the same user name and password as your active Conductor.

You won't need to configure anything. Everything is set up, provisioned, and configured as a standby HA Conductor. The standby Conductor shows **Standby-mode** in the title bar while acting as a standby.

The screenshot shows the Conductor dashboard with the title bar displaying "Standby-mode".

Set up Conductor high availability

To configure Conductor High Availability (HA), you must first complete the initial setup for both Conductors.

Configure the active Conductor

After you have completed initial setup on both Conductors, configure the active Conductor.

1. Log in to the Conductor you want to designate as the active.
2. In **Settings**, go to **Services > Conductor high availability**, and then select **Edit Settings**.



Note: If you don't see it as a choice, select **Add service** and select **Conductor high availability**.

3. Select HA-active in the **Role** drop-down menu and fill in the fields as follows:

- **Local replication IP address** - Enter the IP address of the network adapter on the master Conductor to use to replicate the data to the standby Conductor.
- **Peer replication IP address** - Enter the IP address of the network adapter on the standby Conductor to use to stream the replication data with the master Conductor.
- **Peer Device ID** - To automatically fill this field, select **Load from peer address**.
In v2.2.13 and earlier – Enter the Device ID of the standby Conductor. To locate this ID, log in to the standby Conductor, go to the **Settings** tab, under **Configuration**, copy the **Conductor Device ID**, and paste it into this field on the master Conductor.
- **Airwall Conductor addresses** – Enter the active and standby Conductor IPs or hostnames, or select **Populate from replication IPs**.

Airwall Conductor HA Configuration

Local Airwall Conductor Configuration

Role	Local replication IP address
HA-active	10.7.50.104

HA peer Airwall Conductor configuration

Peer replication IP address	Peer device ID
10.7.50.101	AMA@40130#EC2491F76758
Load from peer address	

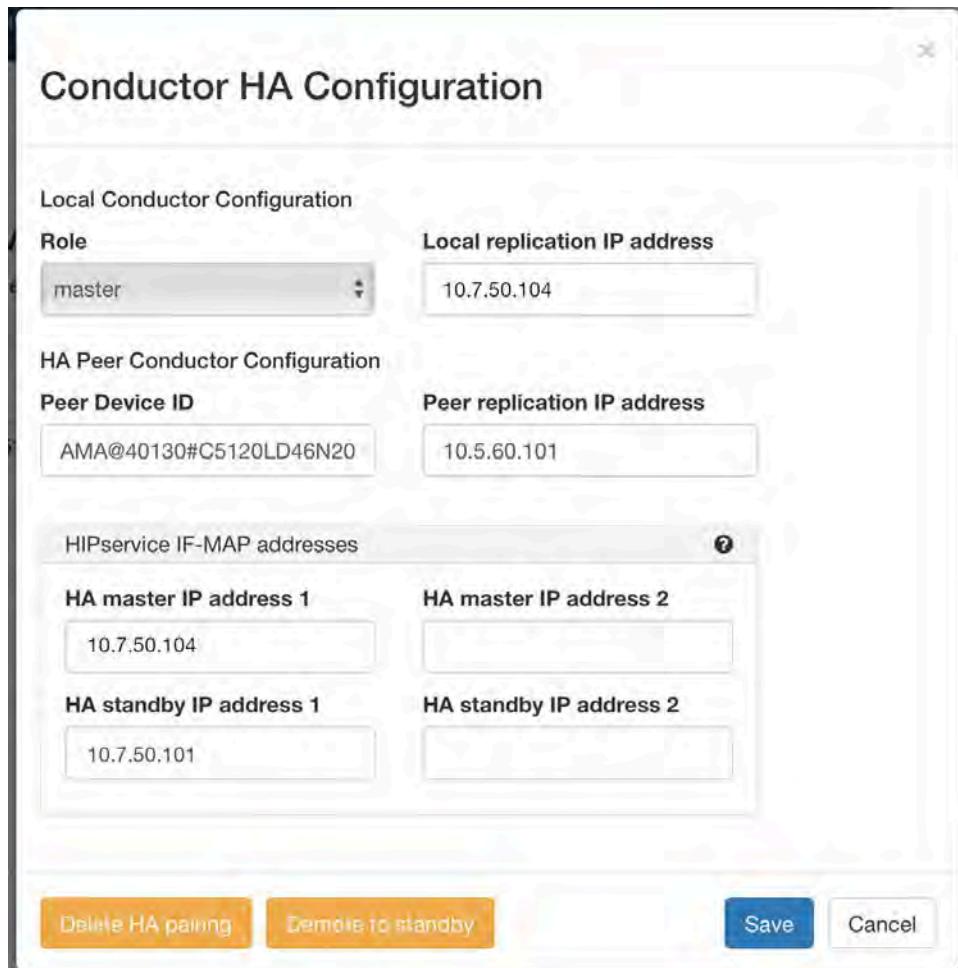
Airwall Conductor addresses	?
Airwall Conductor IP addresses or hostnames +	
pogo1.temperednetworks.com	↑ ↓ Delete
pogo2.temperednetworks.com	↑ ↓ Delete
Populate from replication IPs	

Delete HA pairing **Demote to standby** **Save** **Cancel**

- **For v2.2.13 and earlier:**

- **HA master IP address 1** - Enter the IP address of the active Conductor network interface that Airwall Gateways use to connect to the active Conductor.
- **HA master IP address 2 (Optional)** - If the active Conductor is configured with two network interfaces enabled, enter the IP address of the second network interface of the active Conductor that Airwall Edge Services use to connect to active.
- **HA standby IP address 1** - Enter the IP address of the standby Conductor network interface that Airwall Gateways should connect to if the active Conductor is unavailable.

- **HA standby IP address 2 (Optional)** - If the standby Conductor is configured with two network interfaces enabled, enter the IP address of the second network interface of the standby Conductor that Airwall Edge Services should connect to if the active Conductor is unavailable.



4. Once configured, select **Save**. It may take several seconds to save the active configuration.

Configure the standby Conductor



Note: The standby Conductor inherits the configuration data of the active during the replication process, which erases any existing data on the standby during initial configuration.



Note: For HA pairing, you must have an open TCP port 5432 for Conductor HA communications. For a cloud Conductor, you need to open TCP port 5432 in the cloud provider security group. For a physical Conductor, you must open TCP port 5432 on your firewall.

Once an active Conductor is in place, you are ready to configure the standby.

1. Log in to the Conductor you will use as standby.
2. In **Settings** under **Conductor High Availability**, click **Edit Settings**.
3. Select **HA-standby** in the **Role** drop-down menu and fill in the fields described above for the active Conductor.

After you enter these configuration settings, the standby Conductor connects to the active and initializes data replication. The replication can take a significant amount of time, depending on the number of Airwall Edge Services in the active Conductor database and the network bandwidth available.



Note: After the setup is complete, you may have to re-authenticate.

Once the standby Conductor reboots, it returns you the **Settings** page where it now shows as running in standby mode.



Note: In **Settings** for both the active and standby Conductor, the **Conductor High Availability** section now displays a line indicating if the Conductor is active or standby, and the **Replication Status** displays **Streaming**.

High availability failover for the Conductor

If the master Conductor becomes unavailable, you can switch to the standby Conductor via a manual failover. Failover is performed on the standby Conductor, promoting it to become a master Conductor.

To initiate a failover:

1. Log in to the standby Conductor and go to **Settings**.
2. In the **Conductor High Availability** selection, click **Edit Settings**.
3. In **Conductor HA Configuration**, click **Promote to master** to promote the standby Conductor to the master.

It will take several seconds until the configuration is saved. Once complete, you are redirected to the **Settings** page. Standby mode no longer appears in the top menu and the Conductor's role changes to master in the **Conductor High Availability** section.

Airwall Gateways automatically reconnect to the new master Conductor over time as their connections to the failed Conductor time out. This process may take several minutes and does not affect the operations of the overlay networks.

High availability failback for the Conductor

After a failover has occurred, once the original Conductor becomes available again, or once a replacement is in place, you need to perform a failback to re-establish the high availability pairing.

If a replacement Conductor is required, follow the steps in [Set up Conductor high availability](#) to set up the replacement unit as the new standby Conductor.



Note: If the new Conductor will use different IP addresses than what the failed unit used, you need to re-configure the current active Conductor before proceeding with the failback.

If the original active Conductor can be brought back online without replacing, it can be easily switched to become the new standby. To do this,

1. Log in to the active Conductor,
2. In **Settings**, under **Conductor High Availability**, click **Edit Settings**.
3. In **Conductor HA Configuration**, click **Demote to standby** to transition the Conductor to become the standby.

This Conductor now connects to the active Conductor and initializes the data replication. The replication may take several minutes, depending on the number of Airwall Edge Services in the active Conductor database and the network bandwidth available.

Once you complete the setup, the standby Conductor reboots and you are directed to the **Settings** page.



Note: You may have to re-authenticate on the new standby Conductor once the setup is complete. If the configuration was successful, the Conductor displays standby-mode in the top menu bar.

Breaking a Conductor high availability pair

To break a Conductor HA pair, you first delete the HA configuration on the standby Conductor and then remove the HA configuration on the active Conductor.

To do this, go to **Settings** on the standby Conductor, and in the **Conductor High Availability** section, click **Edit Settings**. In **Conductor HA Configuration**, click **Delete HA pairing** to remove the HA configuration from the Conductor. The Conductors continue to operate, but failover between the two Conductors is no longer enabled.

Update HA-paired Conductors



Note: Conductor High Availability requires port TCP 443 to be open to validate its peer Conductor's version and to send firmware upgrades to the standby.

1. Upload the new Conductor firmware update package to the active Conductor.



Note: The active Conductor sends the firmware update package to the standby Conductor.

2. Update the standby Conductor and wait for the update process to complete.

The standby Conductor is automatically promoted to the active role after the update.

3. Update the active Conductor and wait for the update process to complete.

4. Once both Conductors are updated, demote the designated standby Conductor back to the standby role from **Settings > High Availability**.

Configure Conductor Remote Logging

You can configure the Conductor to send system log messages to a centralized logging service. Your environment must have a syslog service available on the underlay.

Supported Roles

System Administrator



Note: You may need to coordinate with your underlay network administrator to determine the proper syslog service configuration for your environment.

1. Go to **Settings > Services > Remote logging** and select **Edit Settings**.

If you don't see it as a choice, select **Add service** and select **Remote logging**.

2. Select **Enabled** or **Disabled** to turn remote logging on or off.

3. Set the address and port for your remote logging service:

Remote Logging Configuration	
Enabled	Disabled
Remote log service address	mysyslog.com
Port	6514
<input checked="" type="checkbox"/> Log Conductor messages	<input checked="" type="checkbox"/> Use TLS encryption
<input type="checkbox"/> Log Airwall messages	
Additional options	
<input checked="" type="checkbox"/> Log alert notifications	
<input type="button" value="Remove service"/> <input style="background-color: #ffcc00; color: black; border: 1px solid #ffcc00; border-radius: 5px; padding: 2px 10px; font-weight: bold; margin-right: 10px;" type="button" value="Configure"/> <input type="button" value="Cancel"/>	

4. Check whether to use TLS encryption (recommended unless your remote log service is on the same local network as the Conductor). If this box is clear, messages are sent over UDP, which is unencrypted and could introduce a security risk if you are sending the logs over unsecured networks.
5. Check whether to log Conductor and/or Airwall messages, or alerts.
6. Select **Configure**.

Once the logging service is configured and enabled, the Conductor begins to duplicate system log messages and sends them to the configured logging service. Airwall Gateways also obtain the logging service configuration from the Conductor, and will start sending its messages to the logging service if you've configured it to log Airwall Edge Service messages.

Deploy and Configure Airwall Edge Services

Airwall Edge Services let you securely connect managed endpoints, such as laptops, PCs, tablets, and smartphones.

Set up Airwall Gateways

Set up physical, virtual, or cloud Airwall Gateways.

Configure an Airwall Gateway with the `airsh` Setup Wizard

Configure the most common Airwall Gateway setup options using the `airsh` Setup Wizard.

Supported Versions

2.2.10 and later Airwall Gateways

Supported on these Airwall Edge Services

All Airwall Gateways

Before you begin

Collect the following information to set up your Airwall Gateway:

- **Underlay network information** – The protocol (DHCP or static) and type (IPv4 or IPv6) of your underlay network, both wired and Wifi, if enabled. If you are using cell, also your APN (for both modems if you have 2).
- **Conductor address** – The IP address or hostname and port for the Airwall Conductor you want this Airwall Gateway to connect to.
- **Wifi information (if enabled)** – The authentication type, SSID and key for your wireless network.
- **Cellular information (if included)** – Your active carrier, preferred access type (3G or 4G), pin code, authentication type (None, PAP, CHAP, PAP/CHAP), username and password (if applicable), IP connection type (default, IPv4, IPv6, IPv4/IPv6) and whether you want to enable or disable roaming.

Set up an Airwall Gateway with the `airsh` Setup Wizard

1. Connect a computer or [Configure an Airwall Gateway with the `airsh` Setup Wizard](#) on page 237 to access it remotely.
2. Log in to `airsh`. For information on how, see [Airwall Gateway Airshell console commands – `airsh`](#) on page 305.
3. At the `airsh` prompt, enter:

```
setup-ui
```

4. Fill in the information to set up your Airwall Gateway.
5. When you're finished, the status page shows the options you've selected and whether you are connected to your Wifi or cellular network. You may want to note your underlay IPs.

You can reboot to start using the Airwall Gateway, or go into Diagnostic mode to configure more options.

To troubleshoot connection issues, see [Troubleshoot Initial Airwall Gateway connections](#) on page 415.

Set up physical Airwall Gateways

Before you begin installing your Airwall Gateway, ensure that you already have the Conductor installed and configured. After you are finished installing your Airwall Gateway, you can begin connecting devices.



Important: You should familiarize yourself with your model's front panel layout, specifications, power requirements, and safety warnings before use. Also, you should review the procedure for connecting your Airwall Gateway to your Conductor. This information can be found in your model's Platform Guide, included with your Airwall Gateway. If you are unable to locate your Platform Guide, you can download a PDF from the [Documentation Downloads](#) on page 649[Documentation Downloads](#) section of the [Documentation Center](#).

To install and connect Airwall Gateways

To install Airwall Gateways and connect them to the Conductor, you must first apply power to the Airwall Gateway hardware. Once booted, you can configure an Airwall Gateway to connect to the Conductor in one of these ways:

- If your Airwall Gateway has a console port, connect a computer to the console port of the Airwall Gateway, and use `airsh` to configure the Conductor IP address or URL. See [Connect to a physical Airwall Gateway or Conductor with a console port](#) on page 246.

- Put the Airwall Gateway into diagnostic mode and manually configure the Conductor IP address or URL. See [Connect an Airwall Gateway with Diag mode](#) on page 246.
- Configure a DNS SRV record. This might require assistance from your network administrator. See [Connect an Airwall Gateway with a DNS SRV record](#) on page 247.
- Use a factory-configured Conductor URL. This requires assistance from Tempered. See [Connect an Airwall Gateway by using a factory-configured URL](#) on page 248

Insert the SIM card in a 110

Insert the SIM card with the angled corner up, as shown in the first picture.

Correct:



Incorrect:



Set up 75-series hardware

The Airwall Conductor is the central configuration and management point for all Airwall Edge Services. The fastest method to configure and connect your Airwall Gateway to the Conductor is from the console port.

1. Connect the Airwall Gateway to a network shared with the Conductor.
2. Connect a computer to the 75-series Airwall using the micro USB console port located on the back.
3. Using a terminal (macOS, Linux) or terminal emulator (Windows), connect to the Airwall using baud rate 115200.
4. At the login prompt, log in with name: airsh, no password. (For v2.2.3 and earlier, the password is airsh).
5. Use `conductor set` to set the Conductor IP address or URL and port (optional), or remove a Conductor URL. For example: `conductor set my-conductor.tempered`.
6. Turn the power off and back on again.

The Airwall Gateway should now be recognized in the Conductor.

For alternate methods provisioning the Airwall including automatically adding Airwall Gateways as they connect to the network, go to [Connect Airwall Gateways to the Conductor](#) on page 245.

Set up 110-series hardware

[Download PDF](#)

The Airwall 110 platforms are small form factor industrial security appliances that facilitate private overlay networks between customer-provided equipment and devices. This document contains important operating information, specifications, and installation instructions.

SIM Card Orientation

Insert the SIM card with the angled corner up and to the front, as shown in the first picture.

Correct:



Incorrect: Angled edge is inside the slot



Multi-Purpose Button

Also called the Reset button, the multi-purpose button provides two different functions, depending on how long it is pressed and held.

Press Length	Instructions	Function
Short Press	Press for 5 seconds and release. The Status LED will blink steadily.	Places the Airwall Gateway in Diagnostic mode.
Long Press	Press for at least 8 seconds and release. The Status LED will blink in a 2 flash, 1 flash pattern.	Resets the Airwall Gateway to factory defaults.



Note: To exit diagnostic mode, select **Reboot** in the Diagnostic mode interface, or turn the Airwall Gateway off and back on again.

Troubleshooting

If an Airwall Gateway is online, you can use the Conductor to download a packet capture file, a diagnostic report, or a support bundle for troubleshooting. Log in to the Conductor with a system administrator or network administrator account, then go to the Airwall Gateway's **Diagnostics** page: Select **Airwalls**, choose the one you want from the list, then click **Diagnostics**.

Start a packet capture to troubleshoot networking issues:

1. On the Airwall Gateway's **Diagnostics** page, begin a packet capture by clicking **Start Packet Capture**.
2. Stop the packet capture by clicking **Stop Packet Capture**.

You receive a download link once the Conductor has finished creating the packet capture .pcap file. View the .pcap file using any packet-capture and proto-col-analysis tool, such as Wireshark.

Create a diagnostic report to check Airwall Gateway health:

1. On the Airwall Gateway's **Diagnostics** page, you can put it into diagnostic mode and download a diagnostics report. If the Airwall Gateway's is offline, you can put it in **Diagnostics** mode to download the report.
2. Create your report by clicking **Request a diagnostic report**.

You receive a download link once the Conductor has finished creating the report .txt file. Review the diagnostic report for a high-level look at the overall health of the Airwall Gateway.

Create a support bundle for Tempered Support:

A support bundle .pkg file is an encrypted archive that facilitates technical support by Tempered.

1. On the Airwall Gateway's **Diagnostics** page, you can put it into diagnostic mode and download a support bundle. If the Airwall Gateway is offline, you can put it in **Diagnostics** mode to download the support bundle.
2. Create a support bundle by clicking **Request a support bundle**.
3. When the support bundle .pkg file is ready, download the file and send it as an email attachment to support@tempered.io

Fault Relay

This device also has a normally-open relay contact that is connected when the device is fully functional and has underlay connectivity. The relay disconnects when communication via this device is not possible. Connect your custom circuitry bearing in mind the following maximum ratings:

- Voltage: 220 VDC /240 VAC, Max current 2.0A

Specifications

Airwall 110 Series	
Ethernet Ports	2 x 10/100 Mbps RJ-45 ports, auto MDI/MDIX
Console Port	1 x micro USB
Controls	1 x multi-purpose button (actuated with pin)
Indicators	1x Power 1x Status 1x Map / Conductor 1x Diagnostic mode 1x Cellular Link (110g) 1x SIM card (110g)
Relay	Voltage: 220V DC/250V AC, Max current 2.0A
DC Power Input	DC 9-48V, 0.55A-0.1A Over-voltage protection Reverse-polarity protection
Storage Temp range	-45° to 85° C (-49° to 185° F)
Operating Temp range	-40° to 70° C (-40° to 158° F)
Operating humidity	5% to 95% (non-condensing)
Dimensions	31mm W x 100mm D x 125mm H 1.22in W x 3.94in D x 4.92in H
Mounting	DIN-rail, desk-mount
Weight	290g (10.23 oz)
Serial Interfaces	
Protocols	RS-232, RS-485, RS-422

Serial Interfaces	
Connector	2 x DE-9M

Cellular Connectivity (110g)	
SIM card	1x micro (3FF) Push-Push SIM card slot
3G	DC-HSDPA Category 24. 42mbps DL max HSUPA Category 5. 5.76Mbps UL max 24dBm+1dB/-3dB maximum transmit power
4G	LTE Category 4: 1.4 – 20MHz bandwidth FDD 150mbps DL, 50mbps UL max TDD 130mbps DL, 30mbps UL max 23dBm±2dB maximum transmit power
3G bands	WCDMA B1, B2, B4, B5, B6, B8, B19
4G LTE FDD bands	B1, B2, B3, B4, B5, B7, B8, B12, B13, B18, B19, B20, B25, B26, B28
4G LTE TDD bands	B38, B39, B40, B41

Regulatory approvals	
Global	IECEE CB Scheme safety
European Union	LVD, EMCD, RoHS, REACH, WEEE RED (110g)
United States	FCC Part 15B Class A, cULus, FCC Radio
Canada	ICES-03 Class A, cULus, ISED/IC Radio
Japan	VCCI, JATE (110g), TELEC (110g)
Australia	ACMA TLN 2015, RLN 2014, EMR LN 2014 (110g) ACMA EMC LN 2017 (110e, 110g)
New Zealand	Radio Standards Notice 2020 (110g) EMC Standards Notice 2019

Maximum approved antenna gain (dBi, peak)

Band	Uplink Freq (MHz)	USA	Canada	Japan
LTE B12	699 – 716	8.70	7.76	N/A
LTE B28	703 – 748	N/A	N/A	3.00
LTE B13	777 – 787	9.16	8.09	N/A
LTE B5, B19, B20, B26, B18, WCDMA VI	814 – 849	9.36	8.25	3.00
LTE B8	880 – 915	N/A	N/A	3.00
LTE B3, B4	1710 – 1785	5.00	5.00	3.00
LTE B2, B25, B39	1850 – 1920	8.00	8.00	N/A
LTE B1	1920 – 1980	N/A	N/A	3.00
LTE B7, B38, B41	2496 – 2690	8.00	8.00	3.00

Notice:

Hereby, Tempered Networks, Inc declares that the radio equipment type Airwall 110g is in compliance with the Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address:<https://repo.tempered.io/DoC/110>.

The Airwall-110e and Airwall-110g can be used in all EU Member States.

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Radiation Exposure:

This equipment complies with FCC and ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20cm between the radiator and your body and must not be co-located or operating in conjunction with any other antenna or transmitter.

If this device is installed with an antenna other than the type included with it, you must select an antenna and cabling system that respects the maximum antenna gain listed in the tables. If your selected antenna does not meet these criteria, you may void your legal authority to operate this equipment.

Parts List

WALL-HW-110e	Power Supply:
WALL-HW-110g	ACC-HW-110-PSU-25W
included with above:	AC Power cables:
<ul style="list-style-type: none"> • USB A to micro USB cable Micro SIM card slot door • 2x Antennas-ACC-HW-ANT-LTE-5 (ACC-HW-ANT-LTE-3 in Japan) • 1x 3 pin power connector 1x 2 pin relay connector DIN rail mounting kit 	ACC-HW-PWR-C13-NA, (North America) ACC-HW-PWR-C13-JP, (Japan) ACC-HW-PWR-C13-AU, (Australia / New Zealand) ACC-HW-PWR-C13-UK, (UK, Singapore, Malaysia)

Safety and Warnings

DANGER: Elevated Operating Ambient: If installed in a closed environment, make sure the operating ambient temperature is compatible with the maximum ambient temperature specified by the manufacturer.



DANGER: Reduced Air Flow: Make sure the amount of air flow required for safe operation of the equipment is not compromised during installation.



DANGER: Mechanical Loading: Make sure the mounting of the equipment is not in a hazardous condition due to uneven mechanical loading.



DANGER: Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.



Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction

manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Set up Advantech hardware

Airwall Gateway AV3200g firmware can be installed on an Advantech ICR-32xx model routers. The Airwall Gateway firmware supports Ethernet and Cell, as well as Serial port access and Serial over IP. It does not currently support the Wifi or the second SIM socket on this unit. If you're interested in this option, please contact Tempered Sales at sales@tempered.io for licensing information and to get started.

Convert an Advantech ICR-32xx Router into an Airwall Gateway

Supported Versions

2.2.13 Airwall Gateways and Conductor

Requirements

- Advantech Airwall Gateway installer file
- Ethernet connection from your laptop (containing the installer file) to the router
- Advantech Airwall Gateway license

You can convert an Advantech ICR-3241 router into an Airwall Gateway (replacing the Advantech firmware). You can then use it to protect devices and connect to the Conductor for your Airwall secure network as you would with the physical Airwall Gateway hardware available from Tempered.

The Advantech Airwall Gateway firmware currently supports these features in the Advantech hardware:

- Ethernet and Cell
- Serial port access
- Serial over IP

It does not currently support Wi-Fi, or the second SIM socket on this unit.

Convert the Advantech router to an Airwall Gateway

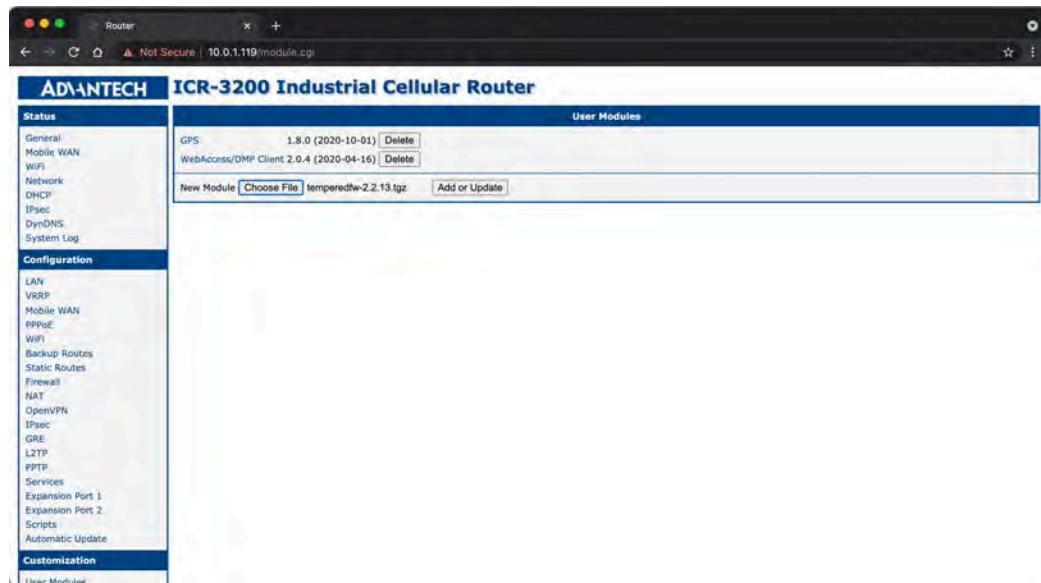
1. Download the latest Airwall Gateway AV3200g firmware installer: [Latest firmware and software](#) on page 431. The Airwall Gateway installer contains Tempered Airwall Gateway and cellular firmware.
2. Connect a laptop that contains the installer file to the Advantech router using an ethernet cable.
3. Log in to the router's web configuration interface using the instructions that come with your router. (The default user is "root" with the unique default password printed on a label on the bottom side of the router.)



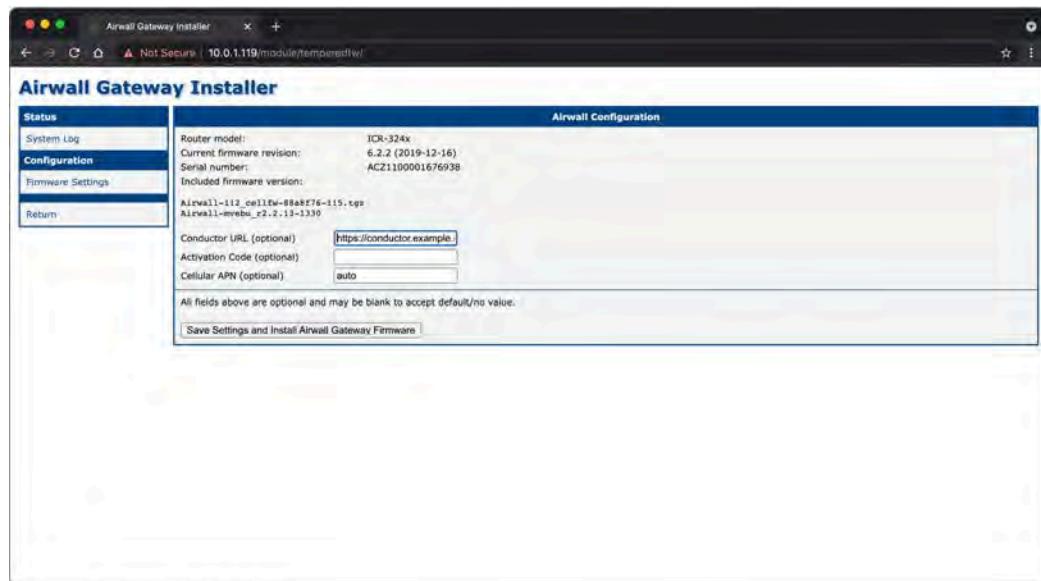
Note: If you need to back up your router configuration, do it before continuing. See your Advantech router instructions for details.

4. On the Advantech router menu, go to **Customization-> User Modules**.

- Select **Choose File**, browse to and select the `temperedfw-2.2.13.tgz` file, and then select **Add or Update**. (The file is about 130 MB and takes about 1 minute to fully upload and unpack.)



- When you get the message that the module upload was successful, select **Back** to return to the list of User Modules.
- In the list, select **Airwall Gateway Installer** to start the install of the Airwall Gateway 3200g firmware.
- When the Installer starts, it opens a page where you can optionally configure your new Airwall Gateway. Enter any settings you want to pre-configure, then select **Save Settings and Install Airwall Gateway firmware**.



- When you get the message that settings (if any) have been saved, select **Install Firmware**.
- Track the install process on the screen. The entire install process should take about 3 minutes.
- When you get the message that the firmware was successfully installed, select **Reboot to Airwall Gateway Firmware**. This reboots the router using the Airwall Gateway firmware.

Once you've installed the Airwall Gateway AV3200g firmware on the Advantech hardware, you can now configure and connect your Airwall Gateway to the Conductor from the console port.



Note: If you pre-configured the Airwall Gateway during installation, you may skip the next section.

1. Connect the Airwall Gateway to a network shared with the Conductor.
2. Connect a computer to the Airwall Gateway using the micro USB console port located on the back.
3. Using a terminal (macOS, Linux) or terminal emulator (Windows), connect to the Airwall Gateway using baud rate 115200.
4. At the login prompt, log in with name: airsh, no password. (For v2.2.3 and earlier, the password is airsh).
5. Use `conductor set` to set the Conductor IP address or URL and port (optional), or remove a Conductor URL. For example: `conductor set my-conductor.tempered`.
6. Turn the power off and back on again.

The Airwall Gateway should now be recognized in the Conductor.

For alternate methods provisioning the Airwall including automatically adding Airwall Gateways as they connect to the network, go to [Connect Airwall Gateways to the Conductor](#) on page 245.

Set Up 100-series Hardware

The Airwall Conductor is the central configuration and management point for all Airwall Edge Services. The fastest method is to connect the Airwall Gateway is from the console port.

1. Connect the Airwall Gateway to a network shared with the Conductor.
2. Connect a computer to the 100-series Airwall using the micro USB console port located on the back.
3. Using a terminal (macOS, Linux) or terminal emulator (Windows), connect to the Airwall using baud rate 115200.
4. At the login prompt, log in with name: airsh, password: airsh.
5. Use `conductor set` to set the Conductor IP address or URL and port (optional), or remove a Conductor URL. For example: `conductor set my-conductor.tempered`.
6. Turn the power off and back on again.

The Airwall should now be recognized in the Conductor.

For alternate methods provisioning the Airwall including automatically adding Airwalls as they connect to the network, go to [Connect Airwall Gateways to the Conductor](#) on page 245.

Set up 200 Series Hardware

Set up 250 Series Hardware

Set up 300 Series for Virtual and Cloud

Set up 400 Series Hardware

Set up 500 Series Hardware

 **Note:** The hardware for an Conductor-500 and an Airwall Gateway-500 are similar. If your order contains both, check the bottom of the unit or the box for a sticker that marks Conductor hardware.

Connect Airwall Gateways to the Conductor

Set up and manage Airwall Gatewaysfrom the Conductor. Before you begin, ensure that you already have the Conductor set up. You can connect the devices that you want to protect to the Airwall Gateway after it is set up.

 **Note:** Please refer to the Airwall Gateway Platform Guide that shipped with your model for additional information and physical port locations.

Once the Airwall Gateway is configured to connect to the Conductor, connect the Airwall Gateway to the underlay on Port 1, or the designated underlay port for your model.

After fully configuring an Airwall Gateway, you can view basic configuration information by navigating to the **Airwalls** tab and selecting an Airwall Gateway. The following information about the Airwall Gateway is available:

- Overlay networks it belongs to
- IP address
- UID (unique ID)
- serial number
- model
- firmware revision
- user authentication (disabled by default)
- encryption (AES-256 (default), AES-128, AES-256 with compression)

Connect an Airwall Gateway with Diag mode

You can manually point an Airwall Gateway to the Conductor URL, depending on your model.



Note: For additional information about manually configuring a URL, see the Platform Guide for your Airwall Gateway model.

1. Connect Port 1 of your Airwall Gateway to a network with access to your Conductor.
2. Configure a computer to use DHCP to obtain an IP address and netmask.
3. Connect the computer to port 2 of the Airwall Gateway.
4. Power up the Airwall Gateway.
5. Place the Airwall Gateway in Diagnostic mode. Use the display screen, if present, or follow the instructions in the Platform Guide for your model. The status LED will display a fast, steady blink pattern in Diagnostic mode.
6. In your web browser, navigate to <http://192.168.56.3> to connect to the Diagnostic mode user interface. It may take a minute for the computer to connect.
7. In **General Settings**, select **Edit Settings**.
8. On the **Edit Airwall Conductor Hostname or IP Setting** page, click the Plus (+) sign.
9. In the **Host** box, enter your Conductor URL or IP address.
10. Click **Submit**.
11. Click **Check** to check your connection to the Conductor.

If you get a "Connection failed" message, it doesn't necessarily mean the connection has failed. If it's yellow, it means unprovisioned, and unlicensed, therefore unable to connect to the Conductor.



Tip: Ping the Conductor IP from the Airwall Gateway to make sure it can reach the Conductor.

12. Reboot the Airwall Gateway. Click **Settings** (gear) icon in the top-right corner of the window, and then click **Reboot**.



Note: You can also reboot turning the Airwall Gateway off and back on.

When the Airwall Gateway comes back online, it contacts the Conductor to request provisioning. To continue, see [Provision and License Airwall Edge Services](#) on page 161.

You can now:

- [Provision and License Airwall Edge Services](#) on page 161.
- Connect the devices you want to protect to the Airwall Gateway. See your platform guide for which port to connect devices to (typically Port 2). For information on adding devices in the Conductor, see [Connect and Configure Devices](#) on page 351

Connect to a physical Airwall Gateway or Conductor with a console port

If your physical Airwall Gateway or Conductor is equipped with a console port (or your cloud or virtual provider allows console access), you can configure the Conductor URL and other options using a computer connected to the console port using `airsh` commands.



Note: For additional information about manually configuring a URL, see the Platform Guide for your Airwall Gateway model.



Note: For more information about the commands available for `airsh`, see [Airwall Gateway Airshell console commands – airsh](#) on page 305.



Note: If you've [Set up Remote Access to Airshell](#) on page 310, you can also [Access an Airwall Gateway Remotely](#) on page 311.

1. **Connect to your network** – Connect Port 1 of your Airwall Gateway to a network with access to your Conductor.
2. **Connect a computer to the Airwall Gateway console port** – Plug in using the micro USB console port. Check your platform guide for the location of your console port, or see [Connecting to the console port on an Airwall Gateway](#) on page 250.
 - a) Using a terminal (macOS, Linux) or terminal emulator (Windows), connect to the Airwall Gateway using baud rate 115200.
3. **Log in to the Console:**
 - v2.2.8 and later: log in with name: `airsh`, and no password
 - v2.2.5 and earlier: log in with name: `airsh`, and password: `airsh`.
4. **Set the Conductor address** - Set the Conductor IP address or URL (and port, if needed (optional)). For example:

```
conductor set my-conductor.tempered.com
```



Tip: Ping the Conductor IP from the Airwall Gateway to make sure it can reach the Conductor.

When the Airwall Gateway comes back online, it contacts the Conductor to request provisioning.

You can now:

- [Provision and License Airwall Edge Services](#) on page 161.
- Connect the devices you want to protect to the Airwall Gateway. See your platform guide for which port to connect devices to (typically Port 2). For information on adding devices in the Conductor, see [Connect and Configure Devices](#) on page 351

Starting with v2.2.8, the Airshell console login has no default password. If you are concerned about securing physical access to Airshell, set a password by entering `conf password` and following the prompts to set and confirm a new password. Keep this password in a secure location, as it cannot be recovered. This password is only for `airsh` physical console access and is not used when you access `airsh` remotely.



CAUTION: If this password is lost, you will need to do a factory reset to clear the password.

Connect an Airwall Gateway with a DNS SRV record

You can connect an Airwall Gateway to the Conductor by using a DNS SRV record.



Note: For specific information, see the Platform Guide for your Airwall Gateway model.

1. **Check DHCP** – Ensure there is a DHCP server and a DNS resolver or DNS server for the local domain accessible from the shared network.
2. **Create a DNS SRV record** – On the DNS server, add a SRV record pointing to the Conductor URL:

```
_service._proto.name TTL class SRV priority weight port target
```

For example, if your shared network domain is `example.com` and the Conductor hostname is `cond-01`, then the SRV record should be:

```
_ifmap._tcp.example.com. 3600 IN SRV 10 0 8096 cond-01.example.com
```



Note: Use the TTL, priority and weight for your DNS environment. Port 8096 is the default, but you can change it in the Conductor and set it to an alternate port.

- 3. Connect to your network** – Connect Port 1 of your Airwall Gateway to a network with access to your Conductor. The DHCP server assigns an IP address, netmask, and a default gateway to the Airwall Gateway. The Airwall Gateway then does a DNS lookup and configures itself using the Conductor address.

You can now:

- [Provision and License Airwall Edge Services](#) on page 161.
- Connect the devices you want to protect to the Airwall Gateway. See your platform guide for which port to connect devices to (typically Port 2). For information on adding devices in the Conductor, see [Connect and Configure Devices](#) on page 351

Connect an Airwall Gateway by using a factory-configured URL

Tempered can pre-configure the Conductor URL for each Airwall Gateway. Airwall Gateways configured with DNS require the user to configure the DNS service to resolve the correct IP address for the Conductor hostname based on the factory-configured URL.

1. Ensure domain name service is configured for your underlay.
2. Apply power to the Airwall Gateway hardware.
3. Connect the Airwall Gateway to your underlay via Port 1 or your underlay port.

You can now:

- [Provision and License Airwall Edge Services](#) on page 161.
- Connect the devices you want to protect to the Airwall Gateway. See your platform guide for which port to connect devices to (typically Port 2). For information on adding devices in the Conductor, see [Connect and Configure Devices](#) on page 351

Check if an Airwall Gateway or Airwall Agent is online

Once an Airwall Edge Service is connected to the Conductor and licensed, you can validate that it is online.

To determine if an Airwall Gateway or Airwall Agent or Server is online:

1. In the Conductor, click **Airwalls** and select the drop-down to the right of the desired Airwall Edge Service.
2. Click **Check online**

If the Airwall Gateway is online, it temporarily displays offline in place of the IP address, then its IP address is displayed in green. If the Airwall Gateway is in fact offline, offline remains in place of the IP address.

Modbus-RTU and Modbus-TCP on an Airwall Edge Service

The Modbus protocol enables data transmission between devices using a serial interface.

Modbus-TCP applies to: 2.1.6 and higher

Beginning with v2.1.6, we have added Modbus support, making it possible to communicate over Internet or Intranet.

The following Airwall Gateways/HIPswitches support Modbus:

- Airwall Gateway-100s (RS-232)
- Airwall Gateway-150 (RS-232)
- Airwall Gateway-250e/g/d (RS-232 & RS-485)
- Airwall Gateway-300 (RS-232)

Modbus-RTU

The Modbus protocol is essentially a technique of enabling data transmission between devices using a serial interface. Our serial-enabled Airwall Gateways have been able to encapsulate Modbus-RTU (Remote Terminal Unit) over a serial line since since firmware 1.x.

With v2.1.6, we have enhanced our Serial over IP (SoIP) feature with Modbus-TCP (Transmission Control Protocol) support making it possible to communicate over Internet or Intranet.

After configuring Modbus via the Airwall Gateway SoIP settings in Conductor, the Airwall Gateway accepts Modbus-TCP commands from servers, issues the commands to serially-connected Modbus RTU devices, and returns

the responses via Modbus TCP back to the server. This configuration provides optimal efficiency for Modbus traffic in terms of throughput, latency, and number of messages as compared to transparent Serial over IP.

Modbus-TCP

Modbus-TCP is a frame-aware Modbus-RTU encapsulation that is compatible with modern Modbus/SCADA systems. Unlike SoIP, Modbus-TCP processes each Modbus frame as a separate packet, and transfers the burden of error correction to the TCP protocol.

Configure Modbus-RTU

Use Modbus-RTU to enable data transmission between devices using the Airwall Gateway serial interface.

1. Connect an RS-232 Modbus Program Logic Controller (PLC) to your Airwall Gateway using a DB9-to-DB9 or DB9-to-RJ45 cable.



Note: RS-485 is supported by the Airwall Gateway/HIPswitch-250, but others will require an adapter.

2. Go to **Airwalls>Airwalls>Ports>Serial over IP**
3. Click **Edit Settings**, and then configure SoIP using the **Generic Serial Over IP** communications protocol.

4. Add the SoIP device to an overlay and create policy.

For information, see [Add devices or device groups to an overlay network](#) on page 355.

5. Using Modbus Polling software, such as [FieldTalk's ModPoll](#), test the configuration using a command such as the following: `modpoll -m rtu -r 1 -c 125 -l -p 4001 10.10.20.162`

Set Modbus-TCP

Use Modbus-TCP now available in firmware 2.1.6 to enable data transmission between devices using the Airwall Gateway serial interface.

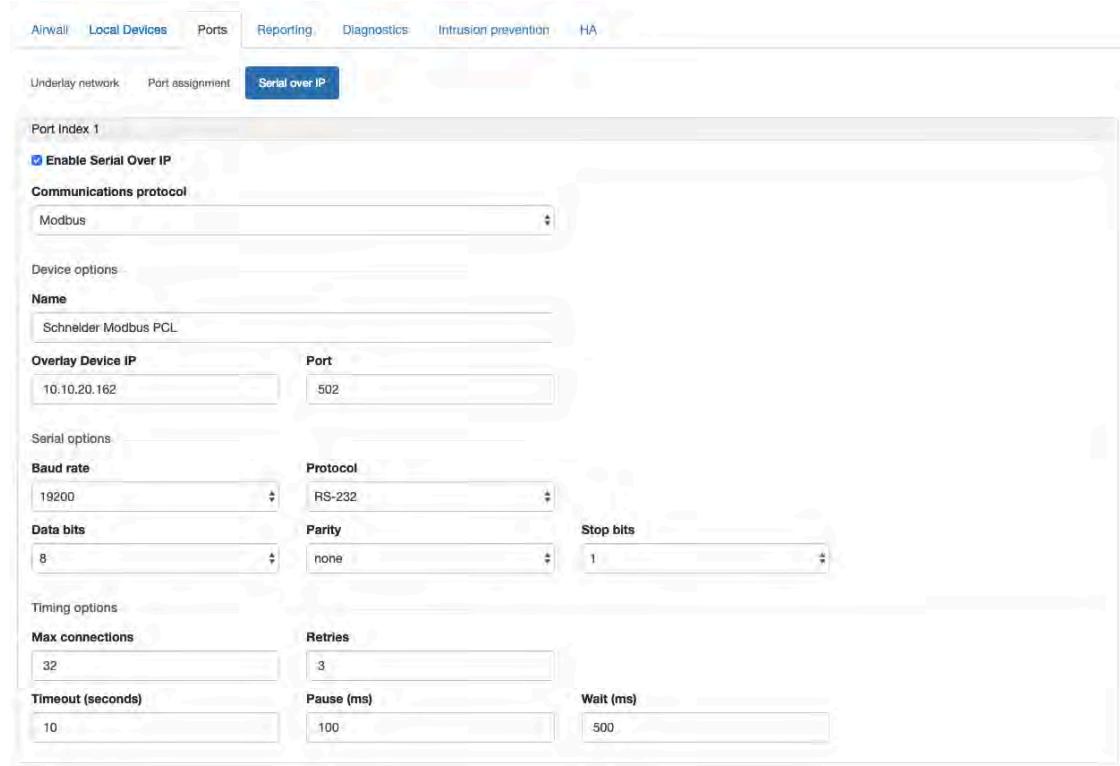
1. Connect an RS-232 Modbus Program Logic Controller (PLC) to your Airwall Gateway using a DB9-to-DB9 or DB9-to-RJ45 cable.



Note: RS-485 is supported by the HIPswitch-250, but others will require an adapter.

2. Go to **Airwalls>Airwalls>Ports>Serial over IP**

- Click **Edit Settings**, and then configure SoIP using the **Modbus** communications protocol.



- Add Modbus-TCP device to the Overlay and create policy

For more information, see [Add devices or device groups to an overlay network](#) on page 355.

- Using Modbus Polling software, such as [FieldTalk's ModPoll](#), test the configuration using a command such as the following: `modpoll -m tcp -r 1 -c 125 -l 10.10.20.162`

Connecting to the console port on an Airwall Gateway

Airwall Gateways with a console port allow you to connect a computer using a cable with a microUSB male connector on one end, and a connector supported by your computer on the other, commonly USB. Once you have connected the Airwall Gateway to your computer and applied power to the device, you can use one of the procedures below to access the Airwall Gateway's configuration options, depending on your computer's operating system.

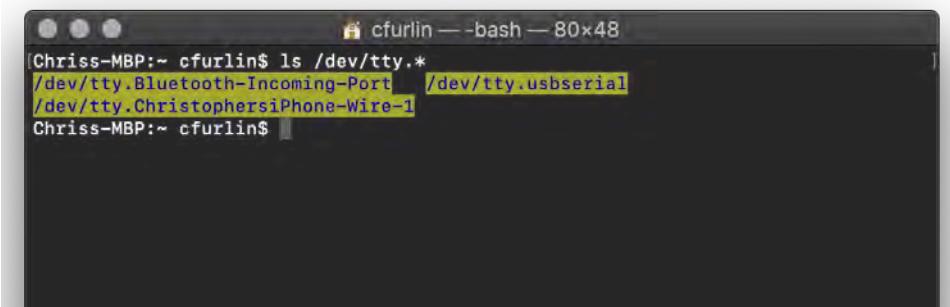
Connect to the console port using Linux or macOS

In a Terminal window, do the following:

- Find the serial interface name. You can look in the dev folder for a `tty*` file, or use `grep tty` and press Enter to obtain the name of the serial interface.



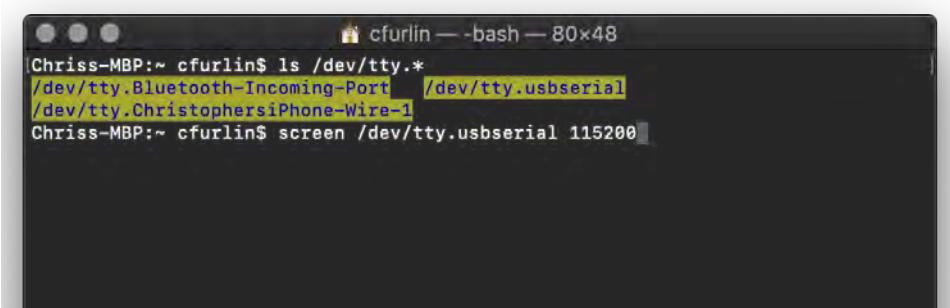
- Locate the interface in the list. In the example below, the interface is /dev/tty.usbserial.



```
[Chriss-MBP:~ cfurlin$ ls /dev/tty.*  
/dev/tty.Bluetooth-Incoming-Port  /dev/tty.usbserial  
/dev/tty.ChristophersiPhone-Wire-1  
Chriss-MBP:~ cfurlin$ ]
```

Note: If you have multiple serial devices attached to your computer, using the command with the Airwall Gateway disconnected and then reconnected may help you determine which interface belongs to the Airwall Gateway.

- Use a TTY terminal app to enter the serial interface and name and baud rate. For example, enter `screen`, the serial interface name, and the baud rate 115200. Press Enter.



```
[Chriss-MBP:~ cfurlin$ ls /dev/tty.*  
/dev/tty.Bluetooth-Incoming-Port  /dev/tty.usbserial  
/dev/tty.ChristophersiPhone-Wire-1  
Chriss-MBP:~ cfurlin$ screen /dev/tty.usbserial 115200 ]
```

- Press Enter again. You may have to do this several times until the login prompt appears.



```
BUD1852000494 login: ]
```

- Log in with username: `airsh` and password `airsh`.
- You can now use `airsh` commands to configure or run diagnostics. The two most commonly used commands are `diag`, which places the Airwall Gateway in diagnostic mode and `conductor set`, which tells the Airwall Gateway where to find the Conductor.

For a list of commands, see [Airwall Gateway Airshell console commands – airsh](#) on page 305.

Connect to the console port using Windows

You can connect to an Airwall Gateway equipped with a console port to configure or run diagnostics using `airsh`.

Note: If you're using an Airwall Gateway running a version earlier than 2.2.3, replace `airsh` with `hipsh` in the instructions below.

- Connect a computer to the Airwall Gateway** – Plug a computer in using the micro USB console port. For the location of the console port, see the platform guide for your hardware.
- Connect to the Airwall Gateway** - Using a terminal emulator, connect to the Airwall Gateway using baud rate 115200.

3. Log in to `airsh` - At the login prompt, log in with: name: `airsh`, password: `airsh`.

You can now run `airsh` commands to configure or run diagnostics on the Airwall Gateway. Examples:

- `diag` - Enter `diag` to put the Airwall Gateway into Diagnostics mode.
- `conductor set` - Set the Conductor URL:

```
conductor set <conductor IP address or URL>
```

For example,

```
conductor set my-conductor.tempered.com
```

For more information, see [Airwall Gateway Airshell console commands – `airsh`](#) on page 305.

Airwall Gateway Platform Guides

Download the latest platform guide for your Airwall Gateway.

Platform Guide	PDF Download Link
Airwall Gateway 75	English
Airwall Gateway 110-series	English French
Airwall Gateway 500-series	English Japanese

110-series Hardware Platform Guide

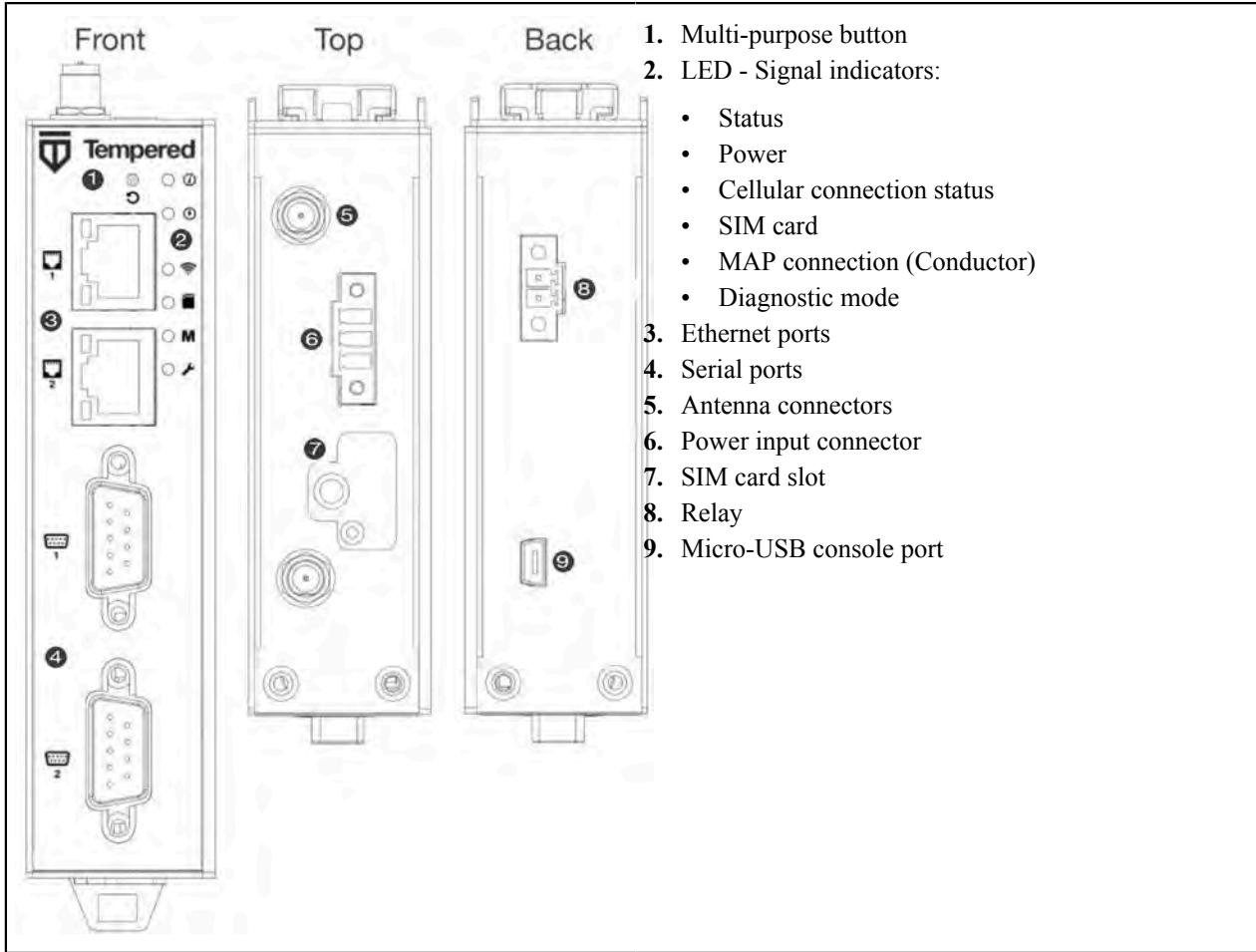
[Download PDF](#)

The Airwall 110 platforms are small form factor industrial security appliances that facilitate private overlay networks between customer-provided equipment and devices. This document contains important operating information, specifications, and installation instructions.

Models

Part Number	Model	Cellular	Eth Ports	Serial Ports
PLF-0138-01	Airwall 110e	No	2	2
PLF-0140-01	Airwall 110g	Yes	2	2

Panel Layouts



Quick Start

- Plug in the Airwall Gateway** – Locate in an area that complies with its safe operating guidelines, and then plug it in or apply power.
- Connect to your network** - Using Port 1, connect the Airwall Gateway to a network where it can reach the Conductor.
- Provide the Conductor address** - There are three ways to configure the Conductor address on the 110-series Airwall Gateways:
 - [Connect an Airwall Gateway with Diag mode](#) on page 246
 - [Connect to a physical Airwall Gateway or Conductor with a console port](#) on page 246
 - [Connect an Airwall Gateway with a DNS SRV record](#) on page 247
- Test your connection to the Conductor** – Check in **Diagnostics** mode, under Airwall Conductor, if the Conductor shows as Reachable, or using the console port, ping the conductor from the Airwall Gateway:

```
ping my-conductor.tempered.com
```

- Connect to devices** – Connect the devices you want to protect to the Airwall Gateway on Port 2.

Status LED Codes

State	LED Pattern	State	LED Pattern
Normal Operation	On Steady	No Conductor Connection	O O O O == O O ==

State	LED Pattern	State	LED Pattern
Conductor Blink	O O ==	System Error	O O O O == O O O ==
Missing Identity	O O O == O ==	Secure Network Error	O O O O ===
Factory Reset	O O == O ==	No Shared Network	O O O O == O ==
Diagnostic Mode	O = O = (fast blink)	Firmware Download	O O O == O O ==
		Firmware Update	O O O ===

Key: **O** is on, **=** is off

Wiring

Power Inputs

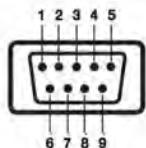
This device supports one power supply. The connector for PWR 1 is located on the terminal block on the top of the unit.



Step 1: Insert the negative DC into the V- terminal and the positive DC into the V+ terminal.

Step 2: To keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-damp screws in the front of the terminal block connector.

Serial Connector



Pin #	RS-232	RS-422	RS-485
1		TX-	Data-
2	RxD	TX+	Data+
3	TxD	RX+	
4		RX-	
5	GND	GND	GND
6			
7	RTS		
8	CTS		
9			

SIM Card Orientation

Insert the SIM card with the angled corner up, as shown in the first picture.

Correct:



Incorrect:



Multi-Purpose Button

Also called the Reset button, the multi-purpose button provides two different functions, depending on how long it is pressed and held.

Press Length	Instructions	Function
Short Press	Press for 5 seconds and release. The Status LED will blink steadily.	Places the Airwall Gateway in Diagnostic mode.
Long Press	Press for at least 8 seconds and release. The Status LED will blink in a 2 flash, 1 flash pattern.	Resets the Airwall Gateway to factory defaults.



Note: To exit diagnostic mode, select **Reboot** in the Diagnostic mode interface, or turn the Airwall Gateway off and back on again.

Troubleshooting

If an Airwall Gateway is online, you can use the Conductor to download a packet capture file, a diagnostic report, or a support bundle for troubleshooting. Log in to the Conductor with a system administrator or network administrator account, then go to the Airwall Gateway's **Diagnostics** page: Select **Airwalls**, choose the one you want from the list, then click **Diagnostics**.

Start a packet capture to troubleshoot networking issues:

1. On the Airwall Gateway's **Diagnostics** page, begin a packet capture by clicking **Start Packet Capture**.
2. Stop the packet capture by clicking **Stop Packet Capture**.

You receive a download link once the Conductor has finished creating the packet capture .pcap file. View the .pcap file using any packet-capture and proto-col-analysis tool, such as Wireshark.

Create a diagnostic report to check Airwall Gateway health:

1. On the Airwall Gateway's **Diagnostics** page, you can put it into diagnostic mode and download a diagnostics report. If the Airwall Gateway's is offline, you can put it in **Diagnostics** mode to download the report.
2. Create your report by clicking **Request a diagnostic report**.

You receive a download link once the Conductor has finished creating the report .txt file. Review the diagnostic report for a high-level look at the overall health of the Airwall Gateway.

Create a support bundle for Tempered Support:

A support bundle .pkg file is an encrypted archive that facilitates technical support by Tempered.

1. On the Airwall Gateway's **Diagnostics** page, you can put it into diagnostic mode and download a support bundle. If the Airwall Gateway is offline, you can put it in **Diagnostics** mode to download the support bundle.
2. Create a support bundle by clicking **Request a support bundle**.

- When the support bundle .pkg file is ready, download the file and send it as an email attachment to support@tempered.io

Fault Relay

This device also has a normally-open relay contact that is connected when the device is fully functional and has underlay connectivity. The relay disconnects when communication via this device is not possible. Connect your custom circuitry bearing in mind the following maximum ratings:

- Voltage: 220 VDC /240 VAC, Max current 2.0A

Specifications

Airwall 110 Series	
Ethernet Ports	2 x 10/100 Mbps RJ-45 ports, auto MDI/MDIX
Console Port	1 x micro USB
Controls	1 x multi-purpose button (actuated with pin)
Indicators	1x Power 1x Status 1x Map / Conductor 1x Diagnostic mode 1x Cellular Link (110g) 1x SIM card (110g)
Relay	Voltage: 220V DC/250V AC, Max current 2.0A
DC Power Input	DC 9-48V, 0.55A-0.1A Over-voltage protection Reverse-polarity protection
Storage Temp range	-45° to 85° C (-49° to 185° F)
Operating Temp range	-40° to 70° C (-40° to 158° F)
Operating humidity	5% to 95% (non-condensing)
Dimensions	31mm W x 100mm D x 125mm H 1.22in W x 3.94in D x 4.92in H
Mounting	DIN-rail, desk-mount
Weight	290g (10.23 oz)

Serial Interfaces	
Protocols	RS-232, RS-485, RS-422
Connector	2 x DE-9M

Cellular Connectivity (110g)	
SIM card	1x micro (3FF) Push-Push SIM card slot
3G	DC-HSDPA Category 24. 42mbps DL max HSUPA Category 5. 5.76Mbps UL max 24dBm+1dB/-3dB maximum transmit power
4G	LTE Category 4: 1.4 – 20MHz bandwidth FDD 150mbps DL, 50mbps UL max TDD 130mbps DL, 30mbps UL max 23dBm±2dB maximum transmit power
3G bands	WCDMA B1, B2, B4, B5, B6, B8, B19
4G LTE FDD bands	B1, B2, B3, B4, B5, B7, B8, B12, B13, B18, B19, B20, B25, B26, B28
4G LTE TDD bands	B38, B39, B40, B41

Regulatory approvals	
Global	IECEE CB Scheme safety
European Union	LVD, EMCD, RoHS, REACH, WEEE RED (110g)
United States	FCC Part 15B Class A, cULus, FCC Radio
Canada	ICES-03 Class A, cULus, ISED/IC Radio
Japan	VCCI, JATE (110g), TELEC (110g)
Australia	ACMA TLN 2015, RLN 2014, EMR LN 2014 (110g) ACMA EMC LN 2017 (110e, 110g)
New Zealand	Radio Standards Notice 2020 (110g) EMC Standards Notice 2019

Maximum approved antenna gain (dBi, peak)

Band	Uplink Freq (MHz)	USA	Canada	Japan
LTE B12	699 – 716	8.70	7.76	N/A
LTE B28	703 – 748	N/A	N/A	3.00
LTE B13	777 – 787	9.16	8.09	N/A
LTE B5, B19, B20, B26, B18, WCDMA VI	814 – 849	9.36	8.25	3.00
LTE B8	880 – 915	N/A	N/A	3.00
LTE B3, B4	1710 – 1785	5.00	5.00	3.00
LTE B2, B25, B39	1850 – 1920	8.00	8.00	N/A
LTE B1	1920 – 1980	N/A	N/A	3.00

Band	Uplink Freq (MHz)	USA	Canada	Japan
LTE B7, B38, B41	2496 – 2690	8.00	8.00	3.00

Notice:

Hereby, Tempered Networks, Inc declares that the radio equipment type Airwall 110g is in compliance with the Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address:<https://repo.tempered.io/DoC/110>.

The Airwall-110e and Airwall-110g can be used in all EU Member States.

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Radiation Exposure:

This equipment complies with FCC and ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20cm between the radiator and your body and must not be co-located or operating in conjunction with any other antenna or transmitter.

If this device is installed with an antenna other than the type included with it, you must select an antenna and cabling system that respects the maximum antenna gain listed in the tables. If your selected antenna does not meet these criteria, you may void your legal authority to operate this equipment.

Parts List

WALL-HW-110e	Power Supply:
WALL-HW-110g	ACC-HW-110-PSU-25W
included with above:	AC Power cables:
• USB A to micro USB cable Micro SIM card slot door	ACC-HW-PWR-C13-NA, (North America)
• 2x Antennas-ACC-HW-ANT-LTE-5 (ACC-HW-ANT-LTE-3 in Japan)	ACC-HW-PWR-C13-JP, (Japan)
• 1x 3 pin power connector 1x 2 pin relay connector	ACC-HW-PWR-C13-AU, (Australia / New Zealand)
DIN rail mounting kit	ACC-HW-PWR-C13-UK, (UK, Singapore, Malaysia)

Safety and Warnings

DANGER: Elevated Operating Ambient: If installed in a closed environment, make sure the operating ambient temperature is compatible with the maximum ambient temperature specified by the manufacturer.



DANGER: Reduced Air Flow: Make sure the amount of air flow required for safe operation of the equipment is not compromised during installation.



DANGER: Mechanical Loading: Make sure the mounting of the equipment is not in a hazardous condition due to uneven mechanical loading.



DANGER: Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.



Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Set up virtual Airwall Gateways

Set up a virtual Airwall Gateway in VMware ESX/ESXi

This section contains instructions to install a virtual Airwall Gateway on the ESXi/ESX (VMware) platform.

Prerequisites

Required licenses

An Airwall 300v license for each virtual Airwall Gateway you are setting up.

You will also need:

- An existing installation of VMware ESX/ESXi server version 6.5.0 and later
- An Airwall Gateway OVA
- The Conductor you are connecting to configured and available

System Requirements

The following VMware ESX/ESXi server hardware is required:

Processor

- Minimum requirement of a single processor with hyper-threading support, VT-x technology, and 64-bit architecture.
- Optimum configuration is minimum 4 processing cores with hyper-threading support, VT-x technology, 64-bit architecture, and AES-NI enabled in the host's BIOS.

Virtual image

Below are the minimum configuration requirements available for a virtual Conductor or Airwall Gateway image:

Platform	Memory	Disk
Conductor	4GB	120GB*
Airwall	1GB	1GB*
Gateway		

* Already included in the default OVA package

Port Group Configuration

By default, a virtual Airwall Gateway OVA image comes with two network interfaces.

Attach each interface to its own port group:

- Port 1 functions as the underlay network
- Port 2 functions as the overlay network

The virtual Airwall Gateway is expandable up to 6 ports. You can configure one port for HA heartbeats with the HA role.

Security configuration

VMware port groups have default security settings inherited from their parent virtual switch. The following port group security settings should be changed to **Accept**:



Note: These changes only need to be made on the port group associated with the overlay device network port group.

- Promiscuous Mode
 - Allows virtual interface adapters connected to this port group to see all Ethernet frames passed on the virtual switch that are allowed under the VLAN policy for the port group.
- Forged Transmits
 - Allows virtual machines to send frames with a MAC Address that is different from the one specified on the virtual interface.

VLAN configuration

- Set **VLAN type** to **VLAN**
- Set a **VLAN ID** unique to this Airwall Gateway overlay device network and protected device



Note: Because virtual Airwall Gateway port groups function as logical groups and not independent network groups, you must set a unique VLAN for each port group attached to an Airwall Gateway.

To deploy the virtual image

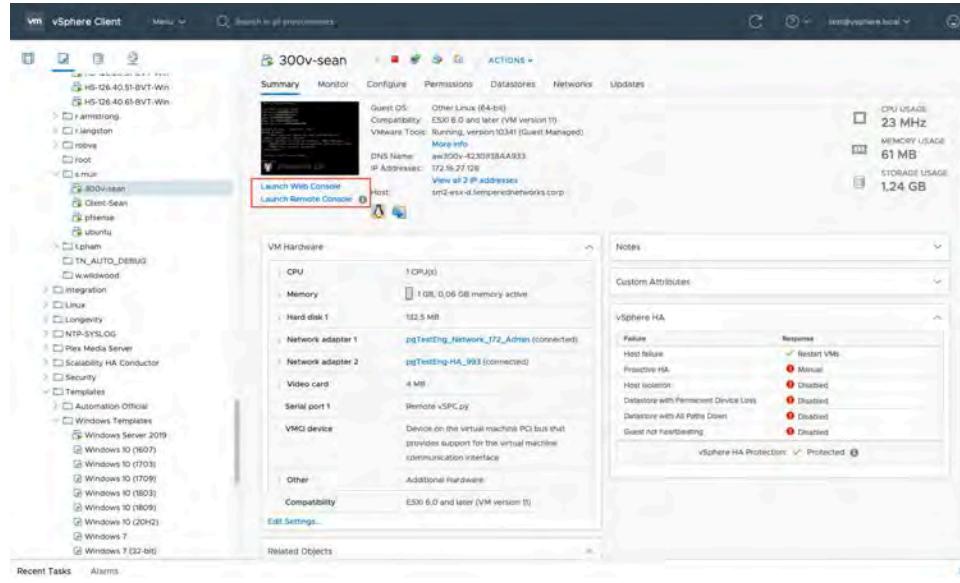
Please check your VMware documentation for the most recent instructions.

1. Download the Airwall x86_64 OVA (ESXi) file from [Latest firmware and software](#) on page 431.
2. Deploy a new OVF template from within ESXi using the downloaded OVA file. For most deployments, you can keep the default settings.
3. Give the virtual machine a unique name and select its storage location.
4. Map the virtual machine's network interfaces with the correctly assigned port groups for the Airwall Gateway.
5. Set **Disk provisioning** to **Thin Provisioned**.
6. Verify your configuration, check **Power on after deployment**, and then select **Finish** to begin the update.

Configure a running Airwall Gateway in VMware ESX/ESXi

Once the Airwall Gateway virtual image is successfully running, you can configure the unit to connect to Conductor. The underlay network interface (port 1) defaults to a DHCP-configured interface.

- In the vSphere ESXi client, select one of the console links:



Launch Web Console opens in a new tab in the browser. **Launch Remote Console** opens in a desktop app that you may need to install.

- On the Airwall Gateway, log in to Airshell with name: `airsh`, and no password (2.2.8 and later).
- You can either determine the IP address for port 1, or manually set it:

- To determine the IP address assigned to port 1, at the Airshell prompt, enter `status network`:

```
airsh> status network
```

- To manually set the IP address for port 1, from the console prompt, enter `conf network` and select 1 to configure the IP. For more help, see [Configure Port Groups with Airshell](#) on page 312:

```
airsh> conf network
```

- Configure the Conductor using `conductor set` followed by the address and port. For example:

```
airsh> conductor set my-conductor.tempered
```

Set up a virtual Airwall Gateway in Microsoft Hyper-V

The virtualization server role for Windows Server 2012 R2 is called Hyper-V Manager. The following documentation show the steps to implement and manage a secure Airwall Gateway and overlay network on Hyper-V network.

Required Licenses

An Airwall 300v license for each virtual Airwall Gateway you are setting up.

Prerequisites

- An existing installation of Microsoft Hyper-V, v2012 or later
- An Airwall Gateway .vhdx file. Download the .vhdx file from [Latest firmware and software](#) on page 431.
- The Conductor you are connecting to configured and available.

Install the Airwall Gateway in Hyper-V

1. Open a Hyper-V Manager Console from within your Windows Machine.
 - **Hyper-V Manager in Windows Server 2012 or Windows Server 2012 R2:**
 - a. In the lower left-corner, select the **Windows** icon.
 - b. Search for **Hyper-V Manager** and open it.
 - **All other versions:**
 - a. Right-click in the lower left-hand corner and select **Run**. Type `virtmgmt.msc` to open the Hyper-V Manager snap-in.
 2. Go to the **Actions** pane and select **New > Virtual Machine** to create a virtual machine for your Airwall Gateway.
-  **Note:** A wizard takes you through the steps to create a **New Virtual Machine**.
3. Select **Specify Name and Location** and give your Airwall Gateway a **Name**.
 4. Leave **Store the virtual machine in a different location** unchecked and click **Next**.
 5. For **Specify Generation**, select **Generation 1**, and select **Next**.
 6. Set the **Startup memory** to *at least* 1 gigabyte of ram (1024).
-  **Note:** Consider how much memory you want to assign your virtual machine, as this is the machine that both contains your data and runs the operating system.
7. Do not check the **Use Dynamic Memory** box. Select **Next**.
 8. In **Configure Networking**, from the **Connection** drop-down, select **Not Connected**. You add this connection later.
 9. Select **Next**.
 10. Under **Connect Virtual Hard Disk**, select **Use Existing virtual hard disk**, browse to the location where you saved the `vhdx` file downloaded from Tempered. Select it and click **OK**.
 11. Click **Next** to complete the set up and view the **Summary** page. You are now ready to add your network adapters.



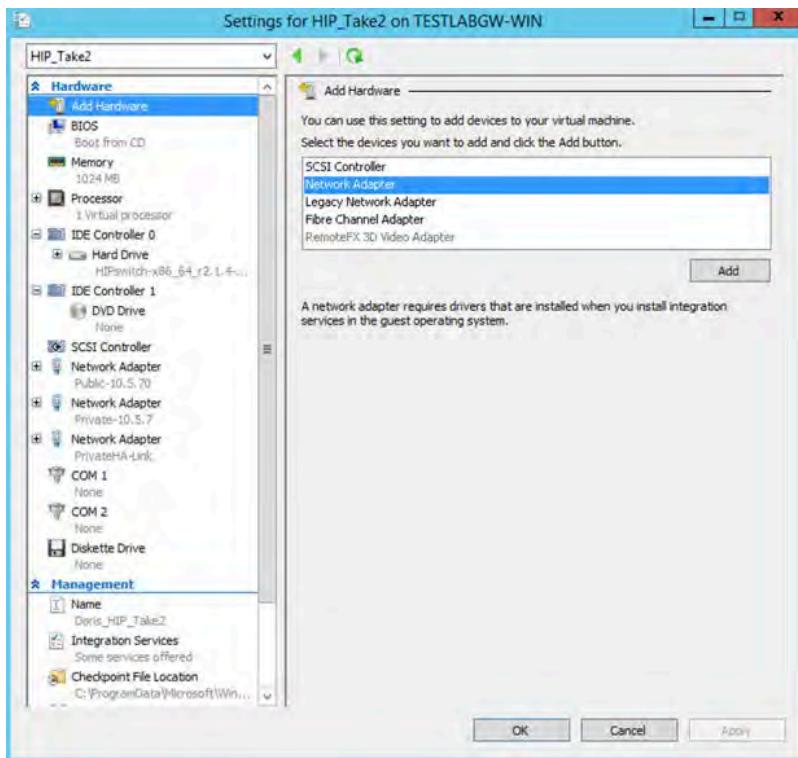
Important: Do not start the machine until you set up the hardware using the procedure below.

Add Network Adapters

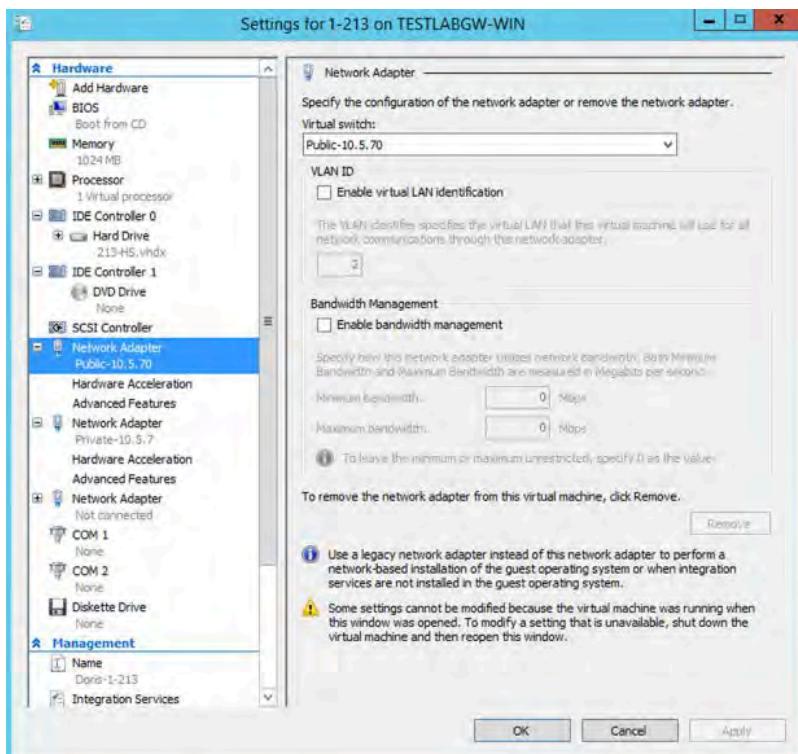
Once you are finished installing the Airwall Gateway software, you are ready to add the network adapters to the machine that will serve as your Airwall Gateway.

1. From the **Virtual Machines** list, find your Airwall Gateway machine and select **Action > Settings**.

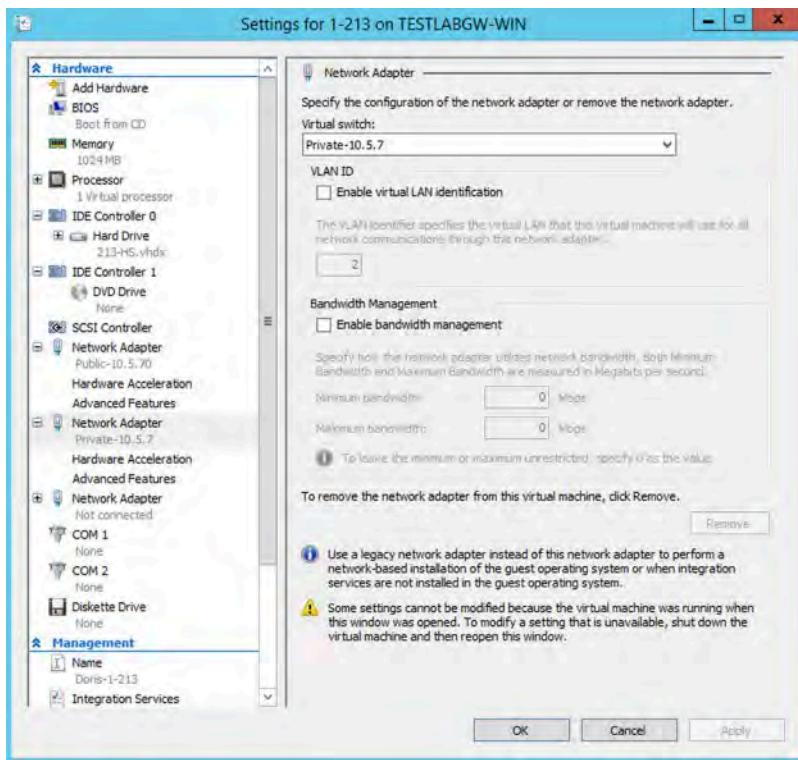
2. Add a minimum of two Network Adapters. To set the first network adapter, select **Add Hardware > Network Adapter** and click **Add**.



3. Configure the first adapter to connect to your underlay. Leave the **VLAN ID** and **Bandwidth Management** options unchecked and click **OK**.

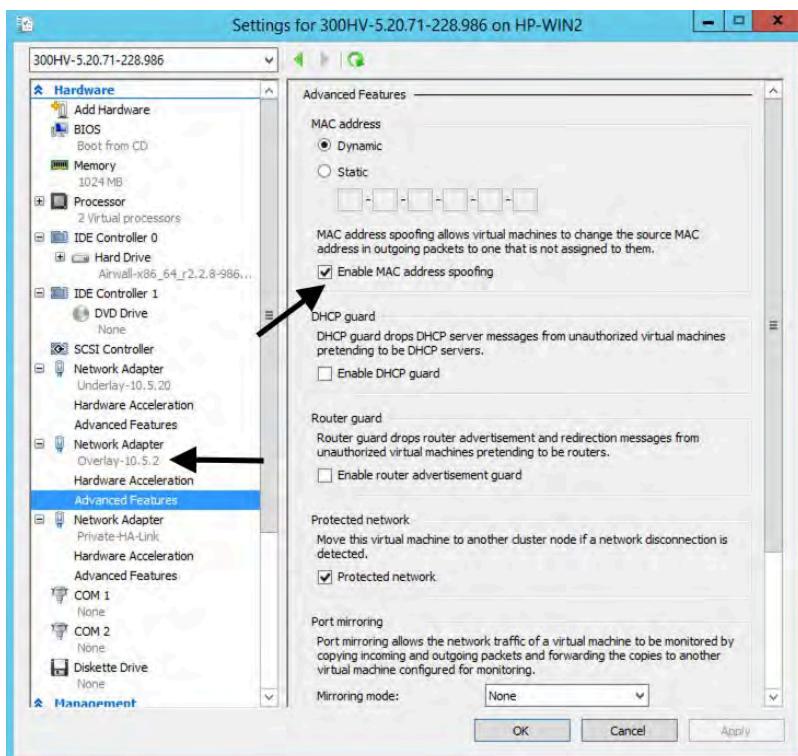


4. Return to **Add Hardware** and configure the second private adapter to connect to your overlay. Leave the **VLAN ID** and **Bandwidth Management** options unchecked and click **OK**.

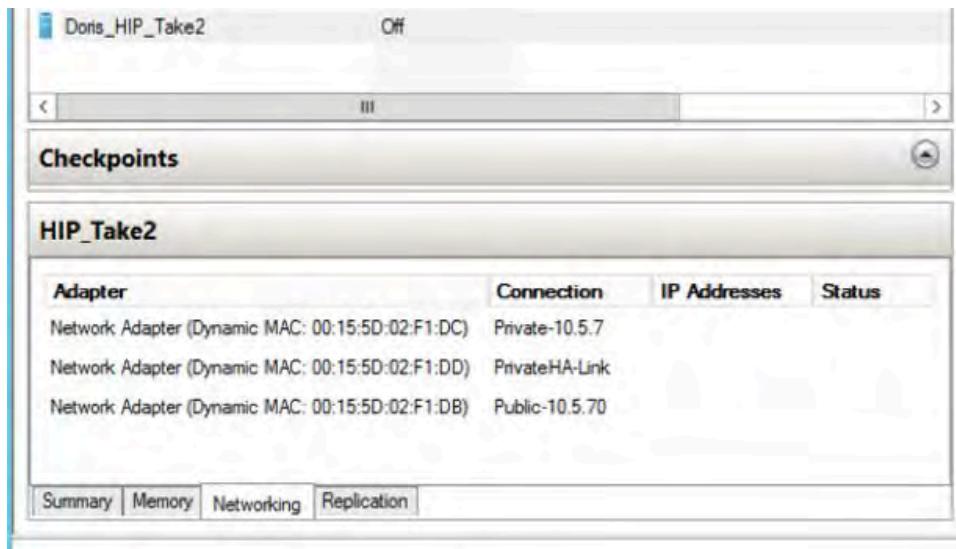


Note: You can have up to two private isolated links. If you are using HA, you can create another adapter and set it to private. For more information on HA, see [Airwall Edge Service High Availability \(HA\)](#) on page 337.

5. Click the plus (next to the overlay Network Adapter, and select **Advanced Features**, and check **Enable MAC address spoofing**.



6. Select the Airwall Gateway machine and open the **Networking** tab to review your settings. Your settings should be similar to this example:



Configure the virtual Airwall Gateway

Connect your virtual Airwall Gateway to your Conductor and configure it.

1. In Hyper-V, select your virtual Airwall Gateway and then select **Action > Connect**.
2. Log in to Airshell.
3. Configure the Conductor and other settings. For more information, see [Configure an Airwall Gateway with the airsh Setup Wizard](#) on page 237.

Expand the Disk Size for a virtual Airwall Gateway

The v3.0 firmware for Airwall Gateways may require more disk space than you currently have allocated on your virtual machines. If so, you get an error message Under **Health data > Reporting** about the disk being too small when you try to update it:

: firmware_verify: Allowing install of upgrade (3.0.0: Airwall-x86_64_r3.0.0-1621)



Important: If you are updating paired High Availability (HA) Airwall Gateways, expand and update the active first, then the standby.

Before you begin

If you have checkpoints for the virtual machines you're expanding, you first need to either delete the checkpoints or clone the virtual machine. For more details on how, see the documentation for your virtual machine software.

Walkthrough – VMware ESXi

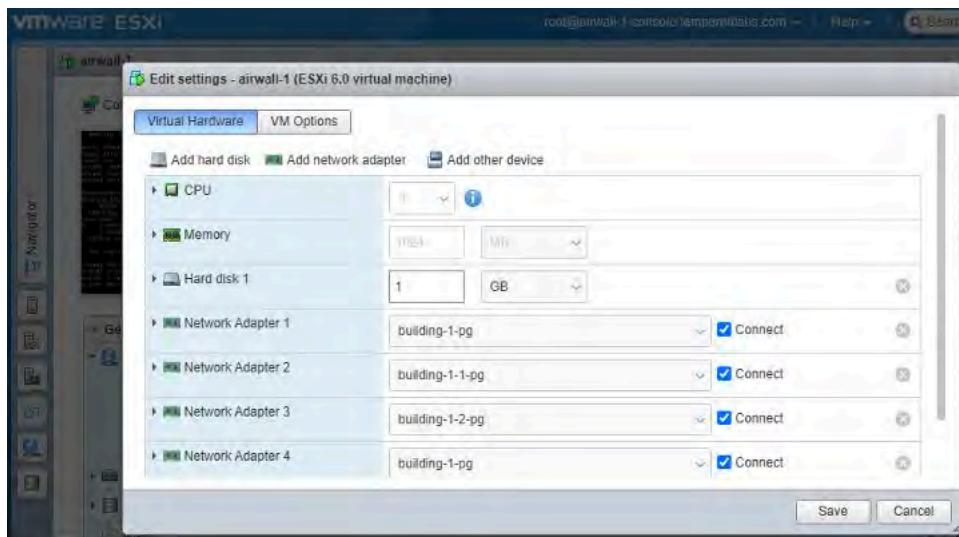
This walkthrough shows how to expand the disk size for a VMware ESXi virtual machine running an Airwall Gateway 300v on the VMware ESXi tool. For more details or updated instructions, see your virtual machine software instructions.

1. Open the VMware ESXi Tool, and select the virtual machine that hosts the Airwall Gateway you want to expand.

- Select **Shut down** to shut down the virtual machine.



- Select Edit.
- Next to **Hard disk 1**, change the size to 1 GB, and select Save.



- Back on the main page, select **Power on** to restart the virtual machine.

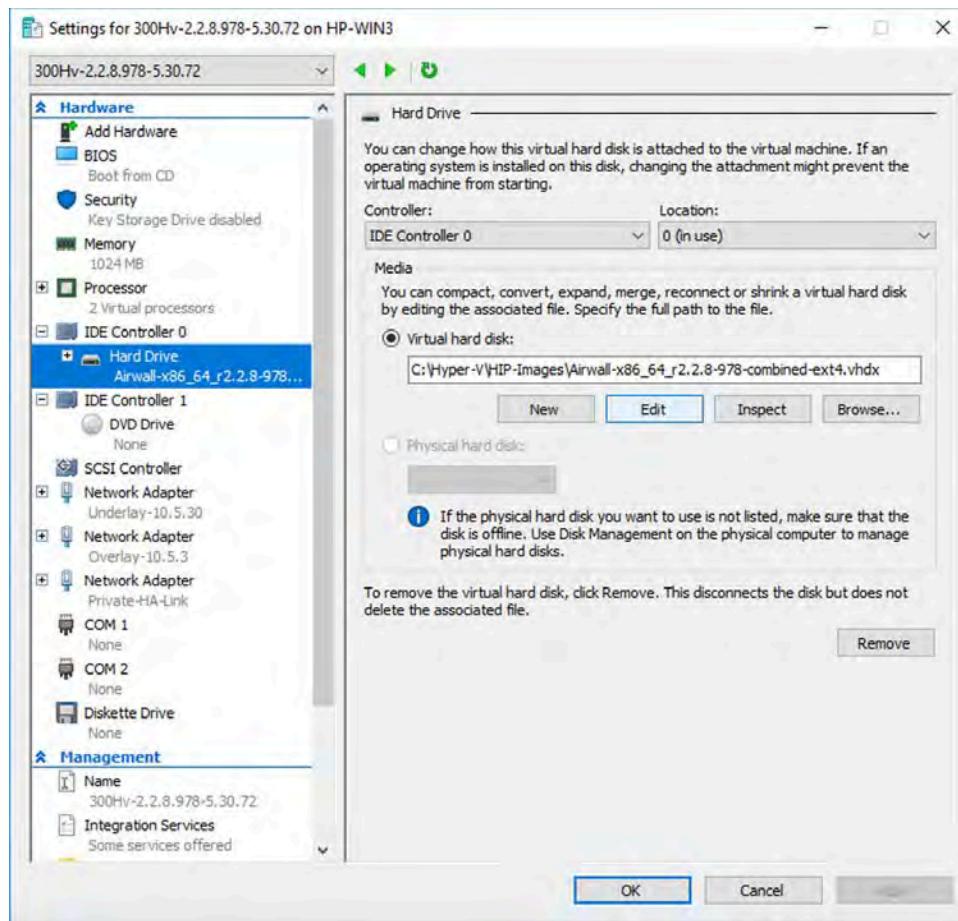
You should now be able to update the firmware for the Airwall Gateway. For help updating firmware, see [Update Airwall Gateway firmware](#) on page 108.

Walkthrough on Hyper-V

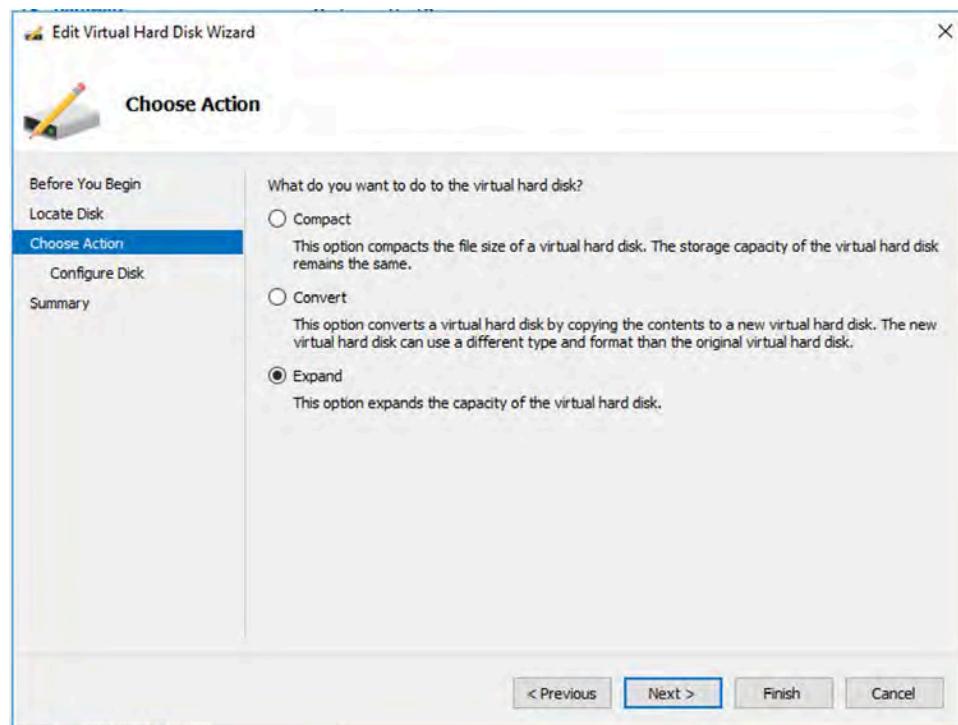
This walkthrough shows how to expand the disk size for a Hyper-V virtual machine running an Airwall Gateway 300v on the Hyper-V Manager v10. For more details or updated instructions, see your virtual machine software instructions.

- Open the Hyper-V Manager, and select the virtual machine that hosts the Airwall Gateway you want to expand.
- Check that the virtual machine has no checkpoints. If it does, delete them or clone the machine to continue.
- Under the actions for the virtual machine, select **Turn Off**, and confirm.
- Select **Settings**.
- Under **Hardware** on the left, select **Hard Drive**.

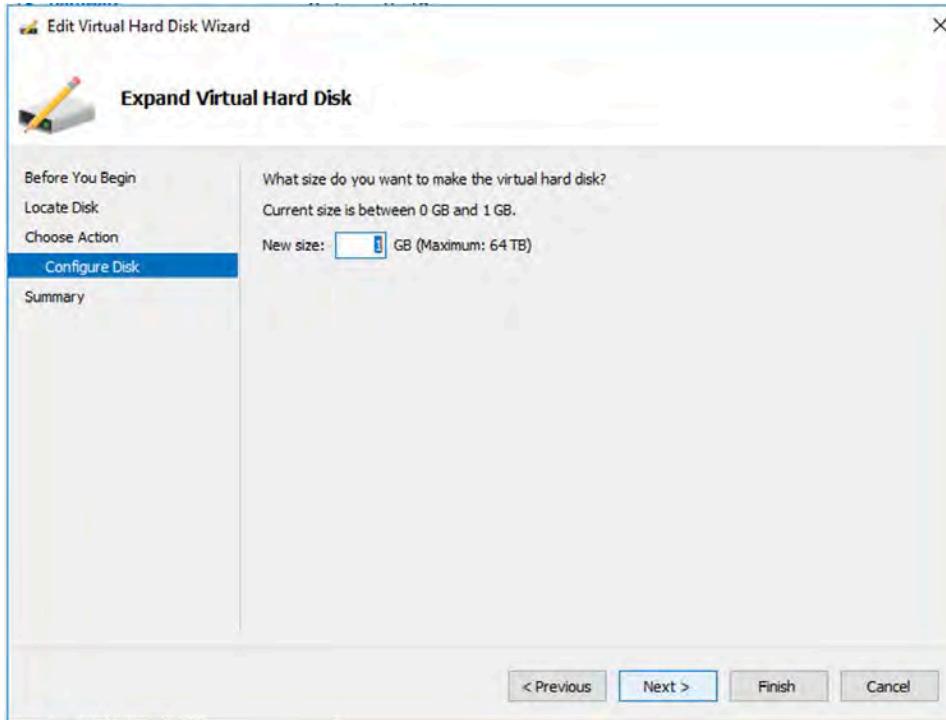
- On the right, under **Media**, select **Edit**.



- On the **Locate Virtual Hard Disk** page, the correct one should already be selected. Select **Next**.
- On the **Choose Action** page, select **Expand**, and then select **Next**.



9. On the **Expand Virtual Hard Disk** page, select 1 GB, and select **Finish**.



10. Back on the main page, restart the virtual machine by selecting **Start** from the lower right menu.

You should now be able to update the firmware for the Airwall Gateway. For help updating firmware, see [Update Airwall Gateway firmware](#) on page 108.

Set up cloud Airwall Gateways

A cloud-based Airwall Gateway provides host-to-host peering between Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and on-premises assets and simplifies the process of managing them.

While you can set up cloud-based Airwall Gateways directly in your cloud platform, the Conductor provides an easy to use user interface for deploying Airwall Gateways in the cloud. Use the links below to view the instructions for each supported platform.

This content assumes you have a good working knowledge of your network and the services you are deploying on. For example, if you plan to deploy an Airwall Gateway in a cloud environment, such as Amazon Web Services (AWS), you should be familiar with the basics of AWS.

Alibaba Cloud – Set up an Airwall Gateway

Once you've set up the Conductor to create Airwall Gateways on Alibaba Cloud, it's easy to create additional Airwall Gateways.

Prerequisites

Required licenses

An Airwall 300v license for each virtual Airwall Gateway you are setting up.

Supported versions

Conductor v2.2.8 and later

To deploy a cloud Airwall Gateway on Alibaba Cloud, you need the following:

- An Alibaba Cloud account, and your access and secret keys.
- The address and port of your Conductor.
- One or more Airwall Gateway image files (from the Alibaba Cloud marketplace, or from Tempered Fulfillment uploaded to the Alibaba Cloud console).

Deploy an Airwall Gateway on Alibaba Cloud

Here's how to deploy an Airwall Gateway to your Alibaba Cloud account:

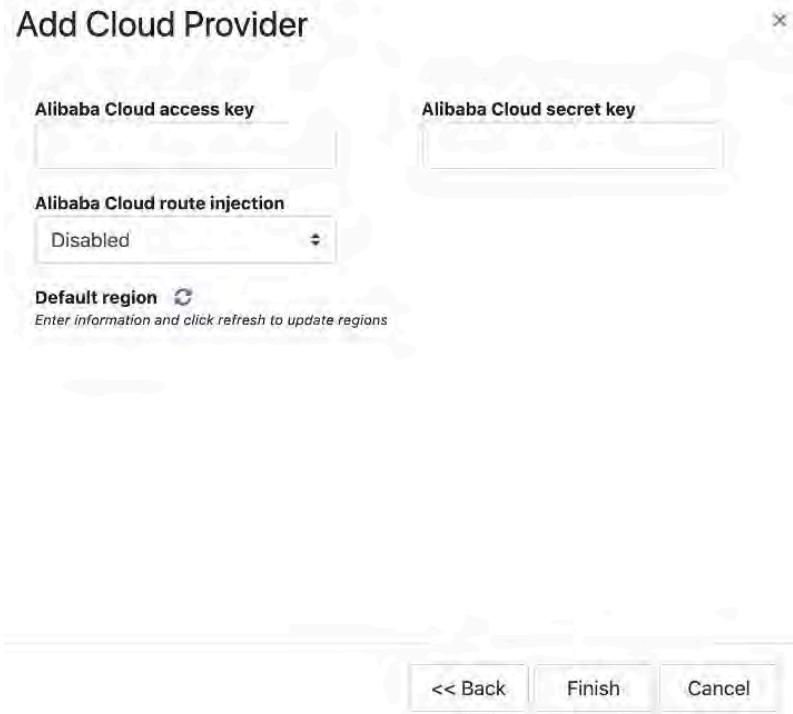
- [Step 1: Add Alibaba Cloud as a provider to your Conductor on page 269](#)
- [Step 2: Create an Airwall Gateway template on Alibaba Cloud on page 270](#)
- [Step 3: Deploy Airwall Gateways on Alibaba Cloud on page 270](#)
- [Step 4: \(Optional\) Change your Elastic IP Bandwidth Setting on page 273](#)

Step 1: Add Alibaba Cloud as a provider to your Conductor

Set up Alibaba Cloud as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

Set up Alibaba Cloud as a cloud provider

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page.
2. Select the **Cloud providers** tab and click **+ Add Cloud Providers**.
3. In the **Add Cloud Providers** dialog, select the check-mark to the right of **Alibaba Cloud** and click **Next**.
4. Enter your **Alibaba Cloud access** and **secret keys**, and choose an option for **Alibaba Cloud route injection**.



5. The **Alibaba Cloud route injection** setting determines how new routes are added to the Alibaba Cloud routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

- If you are using a Airwall Relay, set to **Disabled**.
- If you want to handle traffic for devices individually, set to **Individual traffic**.
- If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.



Note: All traffic is effectively ‘full tunnel’ mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

6. By **Default region**, select the Refresh icon to get the list of regions from the provider, and then select your default region.

7. Click Finish

Your Alibaba Cloud provider is displayed in the **Configured Cloud Providers** list.

Step 2: Create an Airwall Gateway template on Alibaba Cloud

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page, and go to the **Cloud providers** tab.
2. In the **Configured Cloud Providers** list, under **Alibaba Cloud**, select the + next to **Airwall templates**.
3. Give your template a descriptive name, and then select the **Image and network options** you want for Airwall Gateways created with this template.

 **Note:** To select subnets, you need to select a **Network (VPC)** first.

4. Select Save

Step 3: Deploy Airwall Gateways on Alibaba Cloud

You must [Set up Alibaba Cloud as a cloud provider](#) on page 370 before you can add an Airwall Gateway in the Conductor

1. On the **Airwalls** page, (or in Conductor **Settings**, under **Cloud providers**), click **Create cloud Airwall**, and select **Alibaba Cloud Airwall**.



2. In v2.2.8 and later, select the type of Airwall to create, and select **Next**.

3. In v2.2.8 and later, if you want to use a template to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

To continue without a template and enter the information manually, just select **Next**.

- a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.

Create Alibaba Airwall

Name: Alibaba Airwall

Airwall Conductor URL: pogo2.temperednetworks.com:809

Default region: us-west-1

Machine type: ecs.c5.large

Airwall gateway image ID: Tempered Airwall Gateway v2.2.1

Network (VPC): test_network-vpc (vpc-rj9osisqg)

Subnet options

- Public subnet**: test_network-vsw-pub (vsw-rj9C)
- Protected subnet**: test_network-vsw-pro (vsw-rj9b)

<< Back **>> Next** **Cancel**

- b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images available on your cloud provider.
- c) If you don't have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:
- **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
 - **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
 - **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through the Airwall Gateway or through manually-crafted routes.

When you're finished entering the information, click **Create network**, and when processing is complete, click **Back**.

The screenshot shows the 'Create new network (VPC)' section of the 'Create cloud Airwall' interface. It includes fields for 'Network name' (testDocNet), 'Network CIDR' (192.168.0.0/16), 'Public subnet CIDR' (192.168.0.0/24), and 'Protected subnet CIDR' (192.168.1.0/24). A yellow 'Create network' button is at the bottom right, and navigation buttons ('<< Back' and 'Cancel') are at the bottom center.

- d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.
4. Click **Next**.
 5. Check the summary. If everything is correct, click **Create cloud Airwall**.
 6. Click **Finish**. It may take up to 5 minutes for Alibaba Cloud to create the Airwall Gateway.

You've completed creating an Airwall Gateway on Alibaba Cloud, and now need to provision, License, and configure it. For help, see [Provision and License Airwall Edge Services](#) on page 161 and [Configure Airwall Edge Service Settings](#) on page 304.

Step 4: (Optional) Change your Elastic IP Bandwidth Setting

The Airwall Gateway images on Alibaba Cloud use the following default values for elastic IP:

- **Bandwidth:** 5 Mbps
- **InternetChargeType:** PayByTraffic
- **InstanceChargeType:** Postpaid (Pay-As-You-Go)

You can change the bandwidth value once the Airwall Gateway is deployed, however be aware that the bandwidth rate may increase when you edit this value. For more information on how to change the bandwidth, see [Alibaba help](#).

Amazon Web Services – Set up an Airwall Gateway

Prerequisites

Required licenses

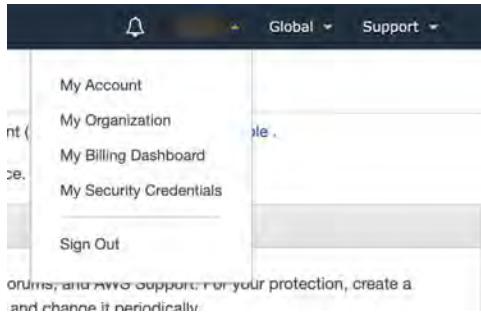
An Airwall 300v license for each virtual Airwall Gateway you are setting up.

Supported versions

Conductor v2.2.3 and later

To deploy a cloud Airwall Gateway on Amazon Web Services (AWS) you need the following:

- An AWS access key ID and secret access key pair to create the AWS cloud provider. If you do not already have a key pair created in your AWS account, you need to create one as follows: Click your username and select **My Security Credentials** in the drop-down.



For more information about access keys, see [AWS Security Credentials](#) in the AWS documentation.



Note: If you create an access key in your AWS root account, you can only retrieve the secret key portion when you create it. If you anticipate using the same key at a later date, we recommend you create an IAM user with access to your security keys instead of relying on root access keys.

- The address and port of your Conductor.
- An Airwall Gateway AMI, shared to your account by Tempered Fulfillment when you purchased your AWS Airwall Gateway.

Set up an Airwall Gateway on AWS

There are three steps required to deploy an Airwall Gateway to your AWS account:

1. Add the AWS provider to your Conductor as a cloud provider
2. Create an Airwall Gateway deployment template
3. Deploy one or more Airwall Gateways using the template

Set up AWS as a cloud provider

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page.
2. Select the **Cloud providers** tab and click **+ Add Cloud Providers**
3. In the **Add Cloud Provider** dialog, select the check-mark to the right of **Amazon Web Services** and click **Next**
4. Enter your **AWS access key**, **AWS secret key**, and **Default region**

The screenshot shows the 'Edit Cloud Provider' dialog box. It has several input fields and dropdown menus. The 'AWS access key' and 'AWS secret key' fields are shown with masked values. The 'AWS route injection' dropdown is set to 'Individual traffic'. The 'Default region' dropdown is set to 'us-east-1' with a checked checkbox. At the bottom of the dialog are three buttons: '<< Back', 'Finish', and 'Cancel'.

5. The **AWS route injection** setting determines how new routes are added to the AWS routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

- If you are using a Airwall Relay, set to **Disabled**.
- If you want to handle traffic for devices individually, set to **Individual traffic**.
- If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.



Note: All traffic is effectively ‘full tunnel’ mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

6. Click Finish

Your AWS cloud provider is displayed in the **Configured Cloud Providers** list.

Configured Cloud Providers	
Amazon Web Services	Create Cloud HIPservice + Add Cloud Provider...
AWS route injection	Disabled
Default region	us-west-1
HIPservice templates +	
Name	Details
<input type="text"/> View	

Create an Airwall Gateway deployment template in AWS

In AWS, create an Airwall Gateway deployment template.

Add an AWS Airwall Gateway

You must [Set up Amazon Web Services \(AWS\) as a cloud provider](#) on page 364 before you can add an Airwall Gateway in the Conductor

1. On the **Airwalls** page, (or in Conductor **Settings** under **Cloud providers** tab), select **New cloud Airwall**, and then select **Amazon Web Services Airwall**.

2. In v2.2.8 and later, select the type of Airwall to create, and select **Next**.

3. In v2.2.8 and later, if you want to use a template to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

To continue without a template and enter the information manually, just select **Next**.

- a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.

- b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images Tempered shared with your account.



Note: If you are not seeing the Airwall Gateway images, check your order email.

- c) If you don't have a pre-configured virtual network, you need to create a new network. Select **Create new network** and fill in the form:

- **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
- **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in AWS.
- **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through the Airwall Gateway or through manually-crafted routes.

When you're finished entering the information, select **Create network**, and when processing is complete, select **Back**.

The screenshot shows the 'Create AWS Airwall' interface. In the 'Create new network (VPC)' step, the 'Network name' is set to 'test-net'. Under 'Network options', 'Network CIDR' is '192.168.0.0/16', 'Availability zone' is 'eu-central-1b', 'Public subnet CIDR' is '192.168.1.0/24', and 'Protected subnet CIDR' is '192.168.2.0/24'. A yellow 'Create network' button is at the bottom right.

- d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.
4. Check the summary and if everything is correct, select **Create cloud Airwall**.
 5. Select **Finish**. It may take up to 5 minutes for Amazon Web Services to complete creating the Airwall Gateway.

You've completed creating an AWS cloud Airwall Gateway, and now need to configure Provision, License, and configure it. For help, see [Provision and License Airwall Edge Services](#) on page 161 and [Configure Airwall Edge Service Settings](#) on page 304.

Microsoft Azure – Set up an Airwall Gateway

You can configure cloud Airwall Gateways on Azure from your Conductor.

Prerequisites

Required licenses

An Airwall 300v license for each virtual Airwall Gateway you are setting up.

Supported versions

Conductor v2.2.3 and later

Before you start, you need

- Access to a Microsoft Azure account with billing set up. If you don't have an account, you can create a free [Microsoft Azure](#) account and upgrade it to a full account later.
- Set up and license an Airwall Conductor.

Create an Azure Application to connect to the Airwall Conductor

Check your Azure documentation for the most recent instructions on creating an application.

1. In Azure, in **Active directory**, under **App registrations**, register or choose an application to act as Airwall API endpoint.
2. In the Azure application, in Certificates & secrets, create a new client secret for the app to connect to Conductor. Copy it to a secure location.



Important: You must copy the new client secret value at this step, because you won't be able to retrieve the key later.

3. From the Azure application you created, note the following information:
 - **Azure Application ID** – Get from the Azure application Overview page.
 - **Azure Application key** – The client secret you noted above.
 - **Azure Subscription ID** – In Azure, under **Users**, get the subscription details to find the ID. It's also at the top of your **Powershell** window.
 - **Directory ID** – Get **Directory (tenant) ID** from the Azure application Overview page.



4. Set up a role for the application you created to use as authorization to create Airwall Gateways in your Azure environment.
 - a) From **Subscriptions**, select your subscription, and then select **Access control (IAM)**.
 - b) Add a role assignment, and assign the App you created to the role: For **Role**, select **Contributor**, and for **Assign access to**, select **User, group, or service principal**, and then search for your App. You can also select a custom role with the permissions you want. For more information, see Azure help: [Create a role in the Azure portal](#).

Accept Azure Terms for the Airwall Gateway Images

Before you can create Airwall Gateways in the Conductor, you'll need to accept terms on Azure for the versions of the Airwall Gateway that you plan to deploy. You only have to accept terms in your current Azure subscription once for each version.

1. In Azure, open **Powershell**.
2. Enter the following command, changing the `--urn` value to the images for the Airwall Gateways you're trying to deploy. For example:

```
az vm image accept-terms --urn tempered-networks-inc:tempered-airwall-v22:tempered-airwall-byol-v22:2.2.3
```

You can get the value you need for `--urn` in the Conductor from the summary page when you are creating the cloud Airwall Gateway. Copy the value for Airwall image ID, and then change the forward slashes to colons. For example, if the drop down list shows an image id of `tempered-networks-inc/tempered-airwall-v22/tempered-airwall-byol-v22/2.2.3`, edit for the `--urn` to `tempered-networks-inc:tempered-airwall-v22:tempered-airwall-byol-v22:2.2.3`.

Add Azure as a Cloud Provider in Conductor

1. In Conductor **Settings**, open the **Cloud providers** tab.
2. Under **Configured cloud providers**, click **Add cloud provider**, and then select **MS Azure**.

3. Fill in the form, using the values noted when creating an application in Azure:
 - **Application ID** – Enter the Azure **Application ID**.
 - **Client secret** – Enter the Azure **Application key**.
 - **Subscription ID** – Enter the Azure **Subscription ID**.
 - **Tenant ID** – Enter the **Directory (tenant) ID**.
4. The **Azure route injection** setting determines how new routes are added to the Azure routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:
 - If you are using a Airwall Relay, set to **Disabled**.
 - If you want to handle traffic for devices individually, set to **Individual traffic**.
 - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.

 Note: All traffic is effectively ‘full tunnel’ mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.
5. For **Default region**, click the **Sync** icon to check the connection and fill in your options. When it connects, select your default region from the list.

Edit Cloud Provider

Application ID	Tenant ID
<input type="text" value="4243d2c6-28ba-4daf-b6aa-7"/>	<input type="text" value="....."/>
Subscription ID	Application key
<input type="text" value="7e1fd3a2-f5b7-49ca-8416-c"/>	<input type="text" value="....."/>
Azure route injection	
<input style="width: 150px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; margin-bottom: 5px;" type="button" value="Individual traffic"/>	
Default region  northeurope	

6. Click **Finish**.

You’re now ready to create cloud Airwall Gateways in Azure in the Conductor.

Add an Azure Cloud Airwall Gateway

You must [Set up Microsoft Azure as a cloud provider](#) on page 365 before you can add an Airwall Gateway in the Conductor

1. On the **Airwalls** page, (or in Conductor **Settings Cloud providers** tab), select **New cloud Airwall**, and then select **Microsoft Azure Airwall**.



2. In v2.2.8 and later, select **Create stand-alone Airwall gateway**, and then **Next**.

3. In v2.2.8 and later, if you want to use a template to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

To continue without a template and enter the information manually, just select **Next**.

- a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.

- b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images available on your cloud provider.
- c) If you don't have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:
- **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
 - **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
 - **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through the Airwall Gateway or through manually-crafted routes.

When you're finished entering the information, select **Create network**, and when processing is complete, select **Back**.

Create Azure Airwall

Create new network (VPC)

Network name
test-net

Network options

Network CIDR 192.168.0.0/16	Availability zone eu-central-1b
Public subnet CIDR 192.168.1.0/24	Protected subnet CIDR 192.168.2.0/24

Create network

<< Back Cancel

- d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.
4. Check the summary and if everything is correct, select **Create cloud Airwall**.
 5. Select **Finish**. It may take up to 5 minutes for Microsoft Azure to complete creating the Airwall Gateway.

You've completed creating an Azure cloud Airwall Gateway, and now need to configure Provision, License, and configure it. For help, see [Provision and License Airwall Edge Services](#) on page 161 and [Configure Airwall Edge Service Settings](#) on page 304.

Provision and License Airwall Edge Services

How to provision and license Airwall Edge Services. You need to [Add Airwall Edge Service Licenses to the Conductor](#) on page 160 before you can provision and license Airwall Edge Services.

1. In Conductor, open **Settings**, and go to the **Licensing** page.
2. If you have a license voucher, [Add Airwall Edge Service Licenses to the Conductor](#) on page 160. If you don't have a license voucher, contact sales@tempered.io to get one before continuing.
3. Install the Airwall Edge Services you want to license and connect them to the Conductor. For more information, see [Deploy and Configure Airwall Edge Services](#) on page 236 and [Connect Airwall Gateways to the Conductor](#) on page 245.
4. Under **Provisioning Requests**, select the check boxes for the Airwall Edge Services you want to provision, and under the **Actions** dropdown, click **Grant Request** to provision your Airwall Edge Services. They should reconnect to the Conductor and appear in your Airwall Edge Services list as unmanaged.



Note: You can also grant provisioning requests from the **Provisioning** tab on the Dashboard.

5. On pre 2.2x Conductors, click **Sync**.
6. On the Conductor dashboard, click the **Show all Airwalls** box and filter the Airwall Edge Services by unmanaged.

- In the row for the Airwall Edge Service you want to license, in the far right column, click the arrow to open the drop down menu, and select **Manage Airwalls**.

Airwall	Model	Status
▶ AW-500 Physical BH@40130#E17C6E5801100057 v2.2.3	Airwall-500 v2.2.3	Online 10.10.24.21
▶ Cloud Airwall Relay Airwall relay BH@40130#EC2397DB7AAE v2.2.3	Airwall-300v v2.2.3	Online 172.16.0.60

Set up an Underlay IP NAT to Connect to your Azure Airwall Gateway

If you want other Airwall Edge Services to be able to connect to your Azure cloud Airwall Gateway, you need to set up a port group on your Underlay to connect to the public IP Azure creates for your Airwall Gateway.

To see if it's set up yet, open the Azure Airwall Gateway in the Conductor. If you see a **Source IP** next to **Online status**, you need to set it up. The public IP is also accessible from the newly created resource group for your Azure Airwall Gateway.

- On the Azure **Airwall** page, on the **Airwall** tab, copy the **Source IP** next to **Online status**.
- Go to the **Ports** tab.
- Open the **Underlay Port group**, and click **Edit Settings**.
- In **Underlay IP (NAT)**, enter the Source IP you copied above.
- Select **Update Settings**.

You now have an Azure cloud Airwall Gateway set up and ready to use.

Troubleshoot Setup on an Azure Cloud Airwall

If you get an “Authorization failed” message when trying to create an Azure cloud Airwall, you need to accept terms for the image you’re using. See [Accept Azure Terms for the Airwall Gateway Images](#) on page 278 .

Google Cloud (GCP) – Set up an Airwall Gateway

Prerequisites

Required licenses

An Airwall 300v license for each virtual Airwall Gateway you are setting up.

Supported versions

Conductor v2.2.3 and later



Note: You should be familiar with using Google Cloud before attempting to deploy a Tempered Conductor or Airwall Gateway on the platform. To get started, we recommend you review the following content offered by Google:

- [Google Cloud Platform Overview](#)
- [Google Cloud Storage](#)
- [Virtual Private Cloud](#)
- [Google Compute Engine Documentation](#)

Set up an Airwall Gateway on Google Cloud

There are three steps required to deploy an Airwall Gateway to your Google Cloud account:

- Set up Google Cloud as a cloud provider
- Add one or more Airwall Gateways

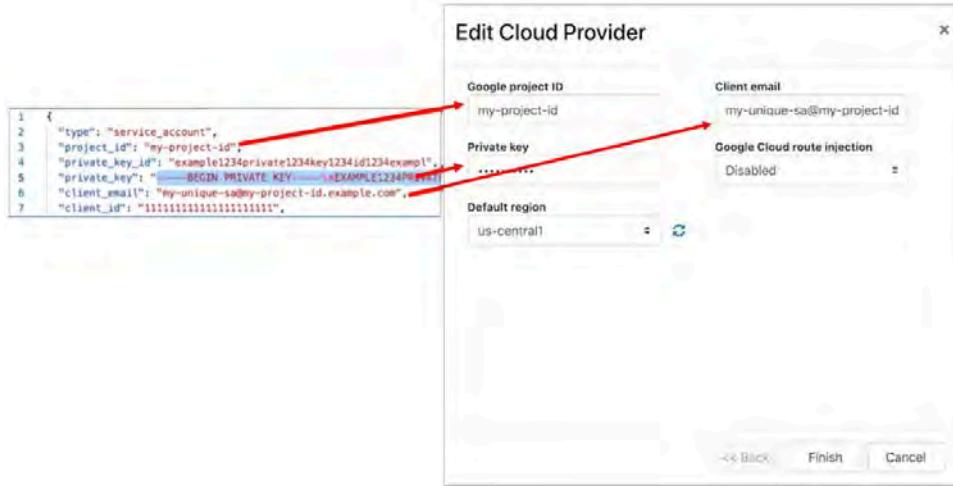
Set up Google Cloud as a cloud provider

- Download a JSON key from your Google Cloud account. For assistance, see Google Cloud help: <https://cloud.google.com/iam/docs/creating-managing-service-account-keys>.



Note: Save the key file somewhere you can access it easily. You will need the information in this file when configuring the Google Cloud provider in the Conductor.

2. Log in to your Conductor, and click the gear icon in the upper right to open **Settings**.
3. On the **Cloud providers** tab, select **Add cloud provider**.
4. Select **Google Cloud**, and then **Next**.
5. Fill in the **Google project ID**, **Client email**, and **Private key** fields with the corresponding information from the key file you downloaded.



6. The **Google Cloud route injection** setting determines how new routes are added to the Google Cloud routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:
 - If you are using a Airwall Relay, set to **Disabled**.
 - If you want to handle traffic for devices individually, set to **Individual traffic**.
 - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.



Note: All traffic is effectively ‘full tunnel’ mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

7. Click **Finish**.



Note: If you need more information about Google Cloud Service Accounts, see <https://cloud.google.com/iam/docs/creating-managing-service-accounts>.

Add a Google Cloud Airwall Gateway

You must [Set up Google Cloud as a cloud provider](#) on page 283 before you can add an Airwall Gateway in the Conductor

1. On the **Airwalls** page, (or in Conductor **Settings Cloud providers** tab), click **New cloud Airwall**, and select **Google Cloud Airwall**.



2. In v2.2.8 and later, select **Create stand-alone Airwall gateway**, and then **Next**.

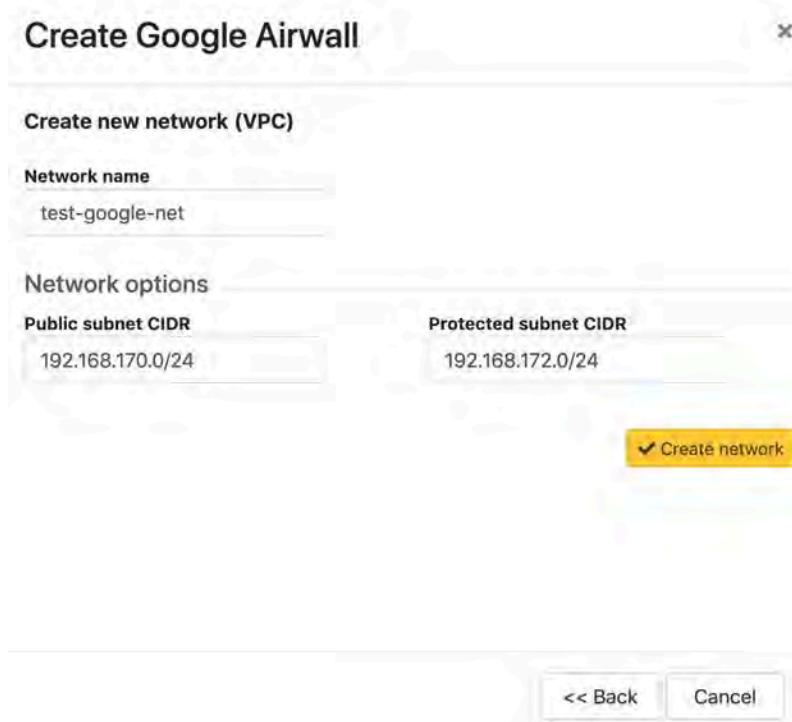
3. In v2.2.8 and later, if you want to use a template to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

To continue without a template and enter the information manually, just select **Next**.

- a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.

- b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images available on your cloud provider.
- c) If you don't have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:
- Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
 - Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
 - Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through the Airwall Gateway or through manually-crafted routes.

When you're finished entering the information, select **Create network**, and when processing is complete, select **Back**.



- d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.
4. Check the summary and if everything is correct, select **Create cloud Airwall**.
 5. Select **Finish**. It may take up to 5 minutes for Google Cloud to complete creating the Airwall Gateway.

You've completed creating a Google cloud Airwall Gateway, and now need to configure Provision, License, and configure it. For help, see [Provision and License Airwall Edge Services](#) on page 161 and [Configure Airwall Edge Service Settings](#) on page 304.

Airwall Gateway for Google Cloud Platform Quick Start

To get started, make sure you have access to your Google Cloud account. If you don't have an account, you can create a free [Google](#) Cloud account and upgrade it to a full account later. If you have an existing Google Cloud account, make sure your billing information is set up. You cannot create a project until you are able to link your billing information to your newly created project.

Step 1: Log in to Google Cloud

From a Web browser, navigate to <https://console.cloud.google.com>. You will see one of two pages, the **Getting Started** page if you have no projects or the **Home** page if you have existing projects.

Step 2: Select the Tempered Airwall Gateway from the Marketplace

You will need to locate the Airwall Gateway in the Google Cloud Marketplace.

1. From your GCP Dashboard, select **Marketplace** on the left sidebar.
2. In the **Search** field at the top of the page, enter `tempered airwall` and press enter.
3. In the results list, locate and select **Tempered™ Airwall**.

This will take you to the product page where you can deploy the Airwall Gateway.



Step 3: Install the Airwall Gateway Image

1. On the product page, click **LAUNCH ON COMPUTE ENGINE**.

2. The Airwall Gateway deployment uses a template so most settings you can leave as is, however you may want to make the following changes:
 - a) **Deployment name:** Enter a name for your Airwall Gateway.
 - b) **Zone:** Select a zone from the drop-down. The zone determines what computing resources are available and where your data is stored and used.
 - c) **Machine type:** Leave as is. Machine type determines the amount of memory, virtual cores, and persistent disk limits for the Airwall Gateway. The default settings are required for the instance to function correctly.
 - d) **Public network:** You can leave the defaults as is and a new network will be created for you. If you have a previously created network you want to use, you can select it here.
 - e) **Networking:** Leave the **Firewall**, and **IP forwarding** fields as is.
 - f) **Protected Network:** This network must be different from the network you selected in the **Public Network** section. In the **Network** drop-down, select **protected**. A new network will be created for you. If you have a previously created network you want to use, you can select it here.
 - g) Click **Show Conductor configuration options** to expose the **Conductor IP Address or Domain Name** field, and enter the address to your Conductor. If you don't know this address, you need to obtain it from the owner of your Conductor. You cannot complete the deployment of your Airwall Gateway without it.



Note: Some fields may be hidden based on your screen size. To view these fields, click **More** button to expand the list.

Deployment name
tempered-hipswitch-v21-1

Zone us-central1-f

Machine type
2 vCPUs 1.8 GB memory Customize

Public Network

Network default

Subnetwork default (10.128.0.0/20)

External IP Ephemeral

Firewall Add tags and firewall rules to allow specific network traffic from the Internet

Allow TCP port 8096 traffic from the Internet
Source IP ranges for TCP port 8096 traffic 0.0.0.0/0, 192.168.0.2/24

Allow UDP port 10500 traffic from the Internet
Source IP ranges for UDP port 10500 traffic 0.0.0.0/0, 192.168.0.2/24

Allow ICMP traffic from the Internet
Source IP ranges for ICMP traffic 0.0.0.0/0, 192.168.0.2/24

[More](#)

Protected Network

Network default

Subnetwork default (10.128.0.0/20)

Conductor Configuration

Conductor IP Address or Domain Name conductor.example.com

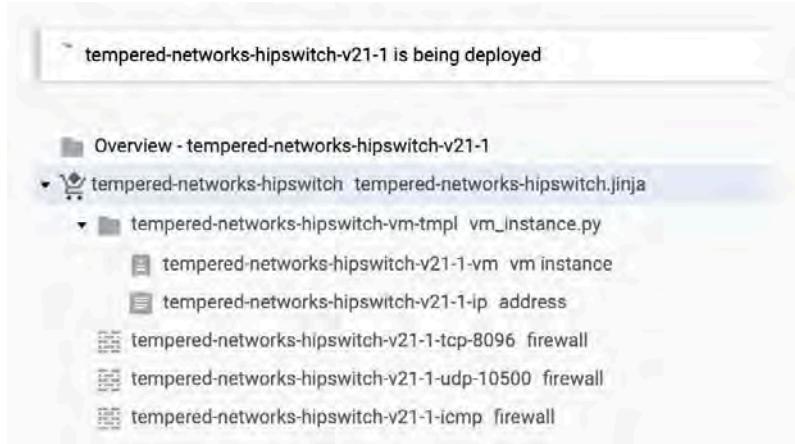
[Less](#)

Deploy

3. Click **Deploy** to begin installing the Airwall Gateway.

Step 4: Finalize the Deployment

It will take a few moments for the process to complete. You can view the progress of your deployment by viewing the tree hierarchy of your components on the page.



Once complete, the message will change indicating your deployment is complete.



Step 5: Verify the Install

At this point the Airwall Gateway instance is running in Google Cloud. It may take several minutes for it to become available after it starts, so if it does not show in the Conductor, try again in a few minutes.

Install Airwall Agents and Servers on people's laptops and devices

How to connect people's cell phones, laptops, and servers to the resources people need access to behind your Airwall secure network.

People connect their devices to your secure network using software installed on their devices. There are Airwall Agent or Server software applications for the most common device types. The easiest way to get your users started is to send them an Airwall Invitation or Activation codes. Help for your users to install the software and connect is here: [Connect to Airwall](#) on page 6.

If you need to install the software from the Conductor, see the unattended installation instructions for select platforms in this section.

Operating system requirements for Airwall Agents and Servers

Operating system requirements for the Airwall Solution and Airwall Teams.T

System Requirements

Please review the system requirements before installing to make sure your device can run the Airwall Agent or Server.

Microsoft Windows

The Windows Airwall Agent works on Microsoft Windows 7, 8.1, or 10, and runs on both Home and Professional versions.

Airwall only: The Windows-based Airwall Server works on Microsoft Windows Server 2008R2, 2012R2, or 2016, or later.

Apple macOS

Works on 10.14 Mojave, or 10.15 Catalina, and later.

Apple iOS

Works on iOS 13 and later. Compatible with the iPhone and iPad.

Android

Works on 6.0 (Marshmallow) and later.

Linux

Works on Ubuntu 16.04, 18.04, and 20.04, and CentOS 8, and (Airwall only) Fedora 2.7.

Raspbian (Raspberry Pi)

Raspbian 9 (Stretch) or 10 (Buster)

RPi4/Ubuntu ARM64 (Raspberry Pi)

Raspbian 10 (Buster)

Microsoft Windows or Windows Server: Install and configure an Airwall Agent or Server

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent or Server for Windows from the administrator of your Airwall secure network, or download the latest installation files from [Latest firmware and software](#) on page 431. Once installed, you configure a profile on the Airwall Agent or Server to link to the Airwall secure network.

 **Note:** You can start and stop the Airwall Agent or Server service as needed. Keep in mind when an Airwall Agent or Server service is stopped, you won't be able to connect to anything on the protected network.

To install and configure the Windows Airwall Agent or Server:

1. Log into your Windows computer as an administrator.
 2. Download and install the Windows Airwall Agent or Server from [Latest firmware and software](#) on page 431.
-  **Note:** If you are asked to install the TAP-Windows Provider as part of the installation procedure, click **Install** when prompted.
3. Once the installation is complete, the Airwall Agent or Server starts automatically.
 4. Right-click the Tempered icon in the Windows System Tray
 5. Select **Configure**
 6. In the **Configure** window, do the following:
 - a) Enter the IP address or host name of your Conductor. The default port setting is *8096*. If you have an activation code, enter it here.

 **Note:** The **Device ID**, **Overlay Device IP**, and **Overlay Netmask** fields are read-only and configurable from the Conductor.

- b) Click **OK**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent or Server is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Windows Airwall Agent or Server, see [Connect with a Windows Airwall Agent or Server](#) on page 27.

 **Note:** You may need to stop and restart the Airwall Agent or Server to allow it to connect to the Conductor. Right-click the Tempered icon in the Windows System Tray and select **Stop** to suspend the service or **Start** to resume.

Unattended Windows installation of an Airwall Agent or Server

In v2.0 and above, you can install the Windows Airwall Agent or Server in unattended mode as an Administrator.

To do an unattended install of the Windows Airwall Agent or Server you use an .msi file. This method runs the regular installer in silent mode, allowing you to do a silent install through domain (GPO, SCCM).

Here's the recommended command to use to do the unattended install:

```
msiexec /i <msi_file> /l*v msi_out.log InvitationCode=<invite_code>
Conductor=<conductor_URL>
```

For example:

```
msiexec /i AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi /
/l*v msi_out.log InvitationCode="575a52703294" Conductor="https://
my.conductor.com:8096"
```



Note: If you are not using DNS, you can replace the Conductor entry with its IP address. For example:

```
msiexec /i AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi /
/l*v msi_out.log InvitationCode="575a52703294"
Conductor="https://192.168.56.2:8096"
```

Apple (OSX and macOS): Install and configure an Airwall Agent

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You must be an administrator of the computer to install and configure the Airwall Agent.



Note: Download the macOS/OSX installation files from the [Tempered Software Downloads and Release Notes](#) on page 431 Software Downloads section of Airwall help.



Important: In v2.2 and earlier, you may be required to install a TAP device driver. In earlier versions, the TAP driver's certificate may display a developer other than Tempered. If this occurs, you can safely click **Allow** and continue with your installation.

Once the installation is complete, the application starts automatically.

To install and configure manually:

1. To install the Airwall Agent locate the files you downloaded, double-click on them to run the installer, and follow the prompts.
2. Left-click the Tempered icon in the macOS menu bar
3. Select **Configure**.
4. On the **Airwall Configuration** page, do the following:
 - a) Select the plus (+) to add a new profile.
 - b) Under **Conductor**, enter the IP address or host name of your Conductor.
 - c) Under **Port**, use the default port setting of *8096*, unless your Airwall secure network administrator has told you to use a different port.
 - d) If you have an Activation code, under **Invitation**, enter the code. If you don't have a code, copy down or screenshot your **Device ID** and send to your administrator to activate your account.



Note: **Device ID**, **Overlay Device IP** and **Overlay Netmask** are read-only and configurable from the Conductor.

- e) Select **Save**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.



Note: You may need to stop and restart the Airwall Agent to allow it to connect to the Conductor. Left-click the Tempered icon in the menu bar and select **Stop Airwall** to disconnect or **Start Airwall** to connect.

For information on using your macOS Airwall Agent, see [Connect with an Apple \(OSX and macOS\) Airwall Agent](#) on page 18.

Perform an unattended macOS installation of an Airwall Agent

In v2.0 and above, you can perform a silent install on the Airwall Agent for macOS.



Note: This action requires administrator rights on the device.

To perform a silent install of the Mac client, from a terminal window, navigate to the location of the Airwall Agent installer package, and enter the command below:

```
sudo installer -pkg ./TemperedNetworkSHIP.pkg -target /
```

Set your preferred network in the macOS Airwall Agent (HIPclient-OSX)

The macOS Airwall Agent (HIPclient-OSX) no longer uses the Network option, but instead automatically uses the network preferences on your macOS system settings.



Note: This action requires administrator rights on the device.

You can change the networks used by the agent by changing your macOS system settings.



Note: This setting is a system-wide setting, and affects network preferences for your entire mac system.

1. On your mac, click the WiFi icon, and select **Open Network Preferences**.
2. Under the list of available networks, click the gear icon, and select **Set Service Order**.
3. Drag the network options to set the network order you prefer, and then click **OK**.

2.2.3 macOS Airwall Agent Upgrade Instructions

If you have a previous version of the macOS/OSX Airwall Agent (formerly HIPclient) installed, follow these instructions to upgrade to 2.2.3:



Note: This action requires administrator rights on the device.

1. Check if you have this file on your Mac: /Applications/TemperedNetworksHIP.app. If not, you can upgrade as normal. If it's there, continue to step 2.
2. In your current Airwall Agent (HIPclient) menu, select **Configure**.
3. Note the Device ID and Conductor URL for each profile.
4. Go to the **About** menu, and select **Uninstall**.
5. Install the 2.2.3 macOS Airwall Agent.
6. Add a new profile for each of the Conductor URLs noted in Step 3. These new profiles will create new provisioning requests for each profile in the Conductor.
7. For the new profiles, a Conductor administrator needs to replace the old profiles with the new profiles. For more details, see [Replace an Airwall Edge Service](#).

Apple iOS: Install and configure an Airwall Agent

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for iOS from Apple's App Store.



Note: If you received an invite, follow the instructions in the email to install and configure your Airwall Agent. The instructions below are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Apple Store: <https://itunes.apple.com/US/app/id1233852249>.
2. Open the Apple iOS Airwall Agent.
3. From the menu, tap **Profiles**. Tap + to add a new profile.

4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it at the bottom.
6. Tap **ADD**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Apple iOS Airwall Agent, see [Connect with an iOS Airwall Agent](#) on page 20.

Android: Install and configure an Airwall Agent

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Agent for Android from the Google Play Store. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.



Note: If you received an invite, follow the instructions in the email to install and configure your Airwall Agent. The instructions below are for manual installation and configuration.

1. Install the Airwall Agent on your device from the Google Play store: <https://play.google.com/store/apps/details?id=com.temperednetworks.hipclient>
2. Open the Android Airwall Agent.
3. Add a new profile:
 - **v3.0 and later** – Scroll down to **Select Profile**, tap **MANAGE**, and then tap **+**.
 - **v2.2.12 and earlier** – From the menu, tap **Profiles**, and then tap **+**.
4. Give the profile a name, and fill in the Conductor URL (and port, if provided to you).
5. If you have an Airwall Invite Code, enter it.
6. Tap **ADD**.

If you've used an Airwall Invitation or Activation code, once the Airwall Agent is recognized by the Conductor, you should be able to start connecting to protected resources. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on using your Android Airwall Agent, see [Connect with a Android Airwall Agent](#) on page 21.

Linux: Install and configure an Airwall Server

If you've received an email or activation code, see [Link my Airwall Agent or Server to an Airwall secure network](#) on page 13. If you need to install and configure manually, follow these instructions. You can get the Airwall Server for your Ubuntu, Centos, or Fedora Linux server from the administrator for your Airwall secure network, or from [Latest firmware and software](#) on page 431. Once installed, you configure a profile on the Airwall Agent to link to the Airwall secure network.



Note:

- For pre-3.0 versions, replace `airsh` with `airctl`.
- For pre-2.2.3 versions, see [pre-2.2.3 help](#).

1. Install the Linux Airwall Server package for your version of Linux. If your secure network administrator has not provided you with a download, you can download the package you need from [Latest firmware and software](#) on page 431.
 - **For CentOS 7 or 8 or Fedora 3.3:** `sudo rpm -i <CentOS or Fedora install package>`
 - **For Ubuntu 16.04, 18.04, or 20.04:** `sudo dpkg -i <Ubuntu 16 or 18 package>`
2. Create a profile: `sudo airsh profile create name=<profile name> conductor=<conductor_url> [act=activation_code]`.
You can optionally enter an Airwall Invitation activation code.
3. Make a profile the active one: `sudo airsh profile activate <profile name or number>`

4. Start the service: `sudo airsh service start`.



Note: If the service is already running, enter `sudo airsh service restart` to stop and start the service.

If you've used an Airwall Invitation or Activation code, once the Airwall Server is recognized by the Conductor, you should be able to start connecting to protected resources on the Airwall secure network. If you are connecting manually, send your Device ID to your administrator so they can activate your account.

For information on getting your Device ID, or using your Linux Airwall Server, see [Connect with a Linux Airwall Server](#) on page 26. For more Airshell commands, see [Linux Airwall Server Airshell commands](#) on page 309.

Linux Airwall Server or macOS Airwall Agent interface selection

The Linux Airwall Server and macOS Airwall Agent implement an interface auto-selection method. When you first install the Airwall Agent or Server, Linux or macOS determines the default gateway of the host and uses the associated network interface.



Note: Auto-selection is per profile.

Troubleshooting

If your Linux Airwall Server or macOS Airwall Agent is reporting as *online*, but doesn't seem to be working, check that the correct network interface is selected in the profile. This can be done by modifying `hip.conf` in the associated profile directory.

Example - List details of the active profile:

```
sudo airctl profile details --active

root@ubuntu-system-files:~# airctl profile details <profile_name>
profile_dir: profile1
profile_name: myprofile
network: ens4
deviceID:
overlay_device_ip:
overlay_mask:
conductor: myconductor.example.com:8096
log_level: info
```

You can find the settings for the active profile in the **profile1** folder under `/opt/tnw/profiles/profile1`. In that folder, open `hip.conf`, and change the `master_interface` key to the network interface you need.

Connect to an Airwall secure network

Once you've installed and linked your Airwall Agent or Server, you can then start and stop it at any time to connect and disconnect from the Airwall secure network.



Note:

- You can use your Airwall Agent or Server to connect to other Airwall secure networks. Just set up a new profile for each one you need to connect to. For information on how, see [Create or Edit Airwall Agent or Server Profiles](#) on page 29
- The Airwall Agent or Server does not disable the wired or wireless interfaces of your device. For example, if you are running an Airwall Agent, you can at the same time be connected to the Internet wirelessly and the corporate network via a wired connection.

Allow an Airwall Agent or Server to access your Airwall secure network

When a person configures an Airwall Agent or Server with your Conductor IP address or hostname, and are online with access to the **Conductor**, their Airwall Agent or Server will appear in the Conductor. How they appear depends on how they've connected:

- If they've activated their Airwall Agent or Server with an Airwall Invitation or Activation code, their Airwall Agent or Server is provisioned and configured as you specified when you set up the invitations or activation codes. You just need to license their Airwall Agent or Server and they will have access to the secure network.
- If the person is connecting manually, you get a provisioning request to allow the Airwall Agent or Server into your secure network. You need to provision and licensed the Airwall Agent or Server, and then add the person's device to the overlay networks and [Add and remove device trust](#) on page 360 for the resources they need access to.



CAUTION: When you're accepting provisioning requests, make sure that you know who is connecting and they are authorized to access your network.

If you need to revoke an Airwall Agent or Server, you can also disable trust in one click. For more information, see [Revoke and Reactivate an Airwall Edge Service](#) on page 419. Open the **Visualization** tab on an overlay network to get a visual view of trust relationships.



Note: You can also automate Airwall Agent trust using the API.

Assign Separate DNS Servers to Airwall Agents and Servers

If you need Airwall Agents and Servers to use different DNS servers, you can assign different DNS servers on an overlay or individually for Airwall Agents and Servers that support it.

Supported Versions

Supported Versions

v2.2.11 and later Conductor, and v2.2.11 and later and Airwall Agents and Servers on platforms that support setting DNS servers (currently macOS, Windows, and Linux). iOS and Android support the global DNS server setting.

Required Role

- System or network administrators
- Permissions to edit the Airwall Agents and Servers or Overlay where you're updating the settings.

Bulk editing supports setting DNS servers on Airwall Agents and Servers.

DNS Setting Priority

The Conductor has a global DNS setting that applies to all Airwall Agents and Servers on your Airwall secure network. You can override the global setting on individual Airwall Agents and Servers, or on an Overlay to apply the DNS setting to all Airwall Agents and Servers that support it on the Overlay.

Here's how the priority is set on DNS settings:

DNS Setting Priority	Result
1 – Airwall Agents and Servers	<ul style="list-style-type: none"> • Overrides the global Conductor DNS server setting. • Can be appended to with DNS Servers set on the Overlay. • Only available on platforms that support the DNS setting (currently iOS, macOS, Windows, and Android). • Will not fall back to the global DNS server setting.

DNS Setting Priority	Result
2 – Overlay	<ul style="list-style-type: none"> Overrides the global Conductor DNS server setting. DNS servers set on the overlay are appended to the end of the DNS Server list set on individual Airwall Agents and Servers. Only applies to Airwall Agents and Servers in the Overlay that support the DNS Server setting.
3 – Conductor Global	<ul style="list-style-type: none"> Applies to Airwall Agents and Servers that both support the DNS setting, and don't have a DNS setting on an Overlay or individually. Is overridden by both Overlay or per-Airwall Agent or Server settings.



Note: MacOS DNS Settings – MAC DNS settings only operate on DHCP interfaces. If your underlay is a static IP, no DNS settings will be applied. At product startup and normal shutdown, DHCP interfaces are returned to DHCP DNS defaults.



Note:

The DNS SRV record covered in [Connect an Airwall Gateway with a DNS SRV record](#) on page 247 is only used for specifying a Conductor URL when deploying Airwall Gateways, and is not related to the DNS Server specified in Conductor settings.

Set DNS servers on an Airwall Agent or Server

This option is only available on v2.2.11 or later Airwall Agents and Servers on platforms that support setting DNS servers, currently macOS, Windows, and Linux.

1. In Conductor, go to **Airwalls**, and open the page for the v2.2.11 or later Airwall Agent or Server for which you want to set the DNS servers.
2. On the **Airwall agent** tab, scroll down to the **DNS servers** line.



Note: If the option is not available, it's not supported on that platform or version.

3. Click the **DNS servers** line to edit.
4. Enter DNS Server IP addresses, separated by commas. For example, enter 8.8.8.8, 4.4.4.4.

DNS servers	8.8.8.8, 4.4.4.4	<input type="button" value="x"/>	<input checked="" type="checkbox"/>
-------------	------------------	----------------------------------	-------------------------------------

5. Select the check mark to save or the X to cancel.

The Airwall Agent or Server now uses the specified DNS servers when connected to the Conductor.

Set DNS servers on an Overlay

Set the DNS servers for all v2.2.11 or later Airwall Agents and Servers in an Overlay that support setting DNS servers.

1. In Conductor, go to an Overlay that has Airwall Agents and Servers for which you want to set DNS servers.
2. On the right, next to **Info**, select **Edit Settings**.
3. Under **DNS servers**, enter DNS Server IP addresses, separated by commas. For example, enter 8.8.8.8, 4.4.4.4.

DNS Server Agents Overlay

Name: DNS Server Agents Overlay

Description:

Manage a relay rule based on this overlay network's configuration

DNS servers: 8.8.8.8, 4.4.4.4

Tags: No entries

Save Cancel

4. Select Save.

The Airwall Agents and Servers on the Overlay that support setting the DNS server now use the specified DNS servers when connected to the Conductor.

Set DNS servers globally in Conductor settings

You can set DNS servers globally in Conductor Settings.

1. In Conductor, open **Settings** and scroll down to **Advanced > Global Airwall agent settings**.
2. Select **Edit Settings**.
3. Next to **DNS servers**, select the plus sign (+) and add the DNS servers you want Airwall Agents and Servers to use.

Advanced

Preferred Airwall agent version: 2.2.8

DNS settings

DNS domain: Apply DNS only when tunnel is active

DNS servers: + 8.8.8.8

Lockdown mode

Enable lockdown mode on compatible Airwall agents

Save Cancel

- If you want to only apply these DNS settings when the DNS servers have an active tunnel, check the **Apply DNS only when tunnel is active** box. See details for this option below.



Note: This setting is currently only supported on the macOS Airwall Agent.

- If desired, enter the **DNS domain** for Airwall Agent overlay DNS Searches. If an Agent is using a per-Agent or Global DNS setting, this global DNS search domain is used (there is no per-agent search domain.)

- Select **Save**.

The Airwall Agents and Servers that support setting the DNS server now use the specified DNS servers when connected to the Conductor.

Details for the **Apply DNS only when the tunnel is active** Setting

The Apply DNS only when the tunnel is active setting does the following:

- If active, DNS is changed to the DNS servers (and search domain) set on the Global DNS settings.
- If no active DNS servers are found, DNS is returned to the DHCP server defaults.
- If an agent DNS is configured (and not available), the global settings are not used.



Note: The DNS servers are pinged at intervals (about half the session expiration time). If a ping brings the tunnel back up, the DNS server setting is applied. If the tunnel goes down, the DNS servers are retested, and DNS returns to the DHCP setting if no servers can be reached. If a tunnel comes up, DNS servers are retested, and it returns to the DNS server setting if at least one of the DNS servers in the list is up.



Note: If you've set separate per-Agent DNS servers and they fail, the agents do not fall back to the global DNS setting.

Automate the Airwall Agent or Server and Airwall Server using the API

Troubleshoot the Airwall Agent and Airwall Server

Follow the instructions below to resolve problems you may encounter using the software.

The Airwall Agent is not connected.

- Determine if the Conductor IP is configured. Follow the steps in the configuration section above.
- Verify that the Airwall Agent has not been given a certificate. Your administrator must grant a license in the Conductor. See the Conductor and Airwall Edge Service Administrator Guide for more information.

The Airwall Agent cannot contact a protected device

Configure the peer Airwall Gateway with an overlay network IP address and reestablish trust.

Deploy a cloud Airwall Server

You can deploy an Airwall Server on a cloud provider, which gives you a Windows Server machine with an Airwall Server installed and configured to connect with your Conductor.

To deploy a cloud Airwall Server, you need to first do the following:

- Set up an Alibaba Cloud, AWS, Microsoft Azure, or Google Cloud account as a cloud provider on your Conductor. See [Set up Cloud Providers](#) on page 364
- Add one or more supported Linux or Windows server VM images to your cloud provider account. See your cloud provider help for instructions. See [Operating system requirements for Airwall Agents and Servers](#) on page 7.
- If you want to automate the provisioning and licensing of the Airwall Server, create an Activation code for it, and enter the code when creating the server.

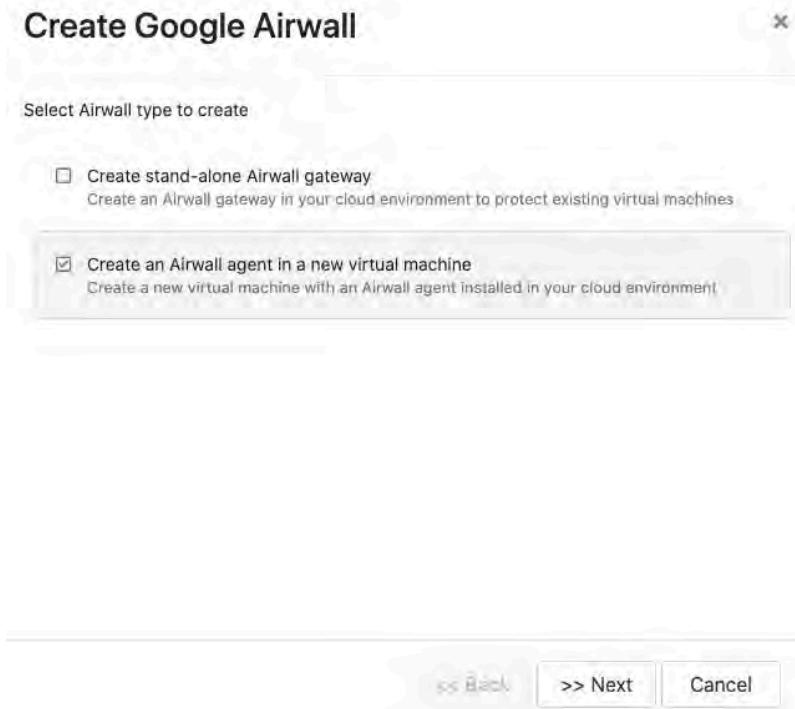
Here's how to deploy an Airwall Server to your cloud provider:

1. On the **Airwalls** page, (or in Conductor **Settings**, under **Cloud providers**), click **Create cloud Airwall**, and select your cloud provider Airwall.

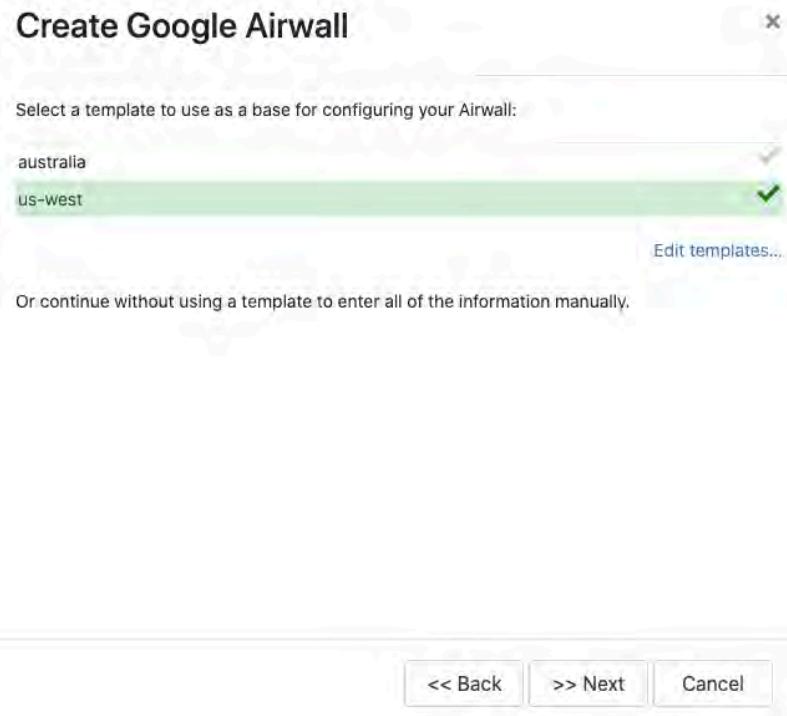


 **Note:** This procedure uses screenshots for Google Cloud, but the process is the same for other cloud providers.

2. Select **Create an Airwall agent in a new virtual machine**, and select **Next**.



3. Select a template, if desired, and then select **Next**.



To continue without a template and enter the information manually, just select **Next**.

4. Give the Airwall Server a descriptive name. If you've used a template, you can skip to the next step.
- a) If you are filling in information manually, or want to change the template, fill in the **Name** and the **Image and network options**. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.

Create Google Airwall

Name: cloud-airwall-server

Airwall Conductor URL: conductor.example.com:8096

Default region: us-west1

Image and network options

- Availability zone**: us-west1-a
- Machine type**: n1-highcpu-2
- Airwall agent VM image ID**: windows-cloud/windows-server-170... (selected)
- Public network (VPC)**: dnt2-public-network
- Create new network**

Subnet options

- Select one...
- dnt2-public-subnet-us-west1** (selected)

<> Back **>> Next** **Cancel**

- b) Under **Airwall agent VM image ID**, pick the type of server you want to create. The list populates with supported Linux and Windows server virtual machine images available on your cloud provider.
- c) If you don't have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:
- Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
 - Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
 - Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through the Airwall Gateway or through manually-crafted routes.

When you're finished entering the information, click **Create network**, and when processing is complete, click **Back**.

Create cloud Airwall

Create new network (VPC)

Network name

Network options

Network CIDR

Public subnet CIDR

Protected subnet CIDR

- d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets.

5. Click Next.

6. Select the package name for the Airwall Server you want to install on the cloud server virtual machine. The package name shows the packages available at the Package URL, which defaults to the Tempered release location.

Create Google Airwall

Image and instance options

Package URL

Package name

Airwall agent options

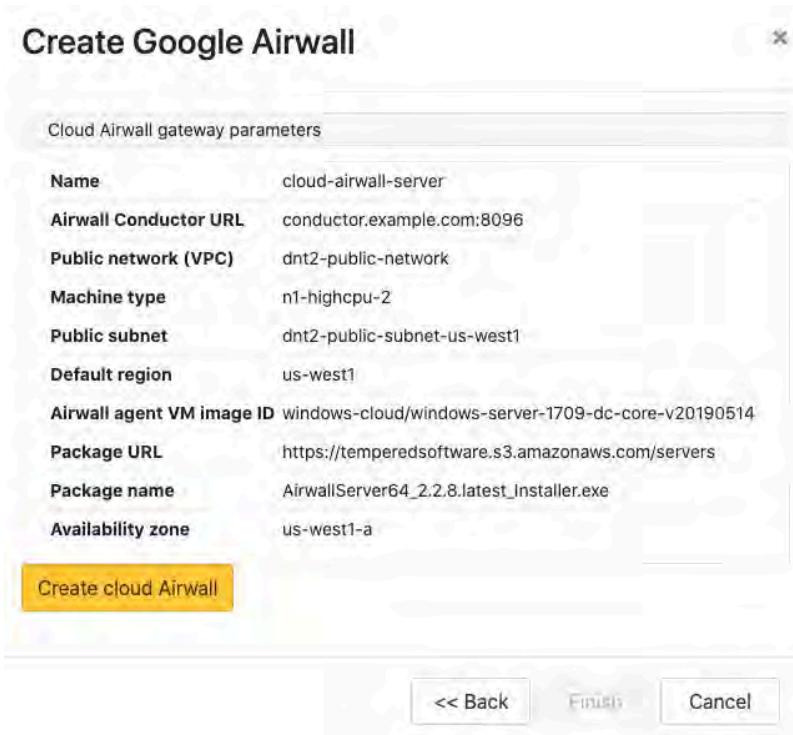
Activation code optional

Custom applications optional

7. If you have an Activation code for the Airwall Server, enter it under Activation code. You can also install custom applications.

8. Click Next.

9. Check the summary of your choices. If everything is correct, click **Create cloud Airwall**.



10. Click **Finish**. It may take up to 5 minutes for your cloud provider to create the Airwall Server.

You've completed creating an Airwall Server on your cloud provider, and may need to provision, License, and configure it. For help, see [Provision and License Airwall Edge Services](#) on page 161 and [Configure Airwall Edge Service Settings](#) on page 304.

Configure Airwall Edge Service Settings

Edit Airwall Gateway settings on **Airwalls edge services** tab. Open the **Actions** menu, select **Properties**, and then **Edit Settings**. After making the desired changes, click **Update Settings**. It may be helpful to assign the Airwall Gateway a human-friendly name.

1. Go to **Airwalls**, select the drop-down to the right of the Airwall Edge Service you want to edit, and select **Properties**.
2. Click **Edit Settings**. You can change the following information:

Basic Settings

- **Name:** A user-friendly name for the Airwall Edge Service.
- **Description:** An optional field for additional information about the Airwall Edge Service.
- **Location:** An optional field for information of about the Airwall Edge Service location.

Advanced Settings

- **Network policy communications:** Enable or disable communication with the Airwall Edge Service.
- **Shared network public IP address (NAT):** If the Airwall Edge Service has a public IP address on the Internet, enter it here. Remote Airwall Edge Services can use this address to connect to the Airwall Edge Service.

- **Enable auto-connect:** If enabled, the Airwall Edge Service securely connects to peer Airwall Edge Services without the presence of device traffic.

3. When finished, click **Update Settings**.

[Set a Private APN for your Cellular Provider on an Airwall Gateway](#) on page 313

You can set the APN of the cell modem on an Airwall Gateway (100, 110, 150, 250) on the Airwall Gateway from Diagnostic mode or using `airsh`, or from the Conductor.

Airshell Command Line

The Airshell command line allows you to manage certain aspects of Airwall Gateways and Airwall Servers from the command line.

Airwall Gateway Airshell console commands – airsh

For Airwall Gateways that have a console port, you can deploy and configure the Airwall Edge Service with the **Airshell** (`airsh`) command-line interface. `airsh` provides tab-completion, inline help, and the ability to deploy & configure directly without going into diagnostic mode.

Connect a computer to the console port on the back of the Airwall™ or Conductor hardware, and use a terminal (macOS, Linux) or terminal emulator (Windows) to open the console. See the platform guide for your Airwall for specific connection instructions.

To access Airwall Gateways with `airsh` remotely, see [Set up Remote Access to Airshell](#) on page 310.

At the console:

- v2.2.8 and later: log in with name: `airsh`, and no password
- v2.2.5 and earlier: log in with name: `airsh`, and password: `airsh`.

You can then enter commands at the `airsh>` prompt.



Note: See also [Linux Airwall Server Airshell commands](#) on page 309.

No Default Password in v2.2.8 and later

Starting with v2.2.8, the Airshell console default login has no default password. If you are concerned about securing physical access to Airshell, set a password by entering `conf password` and following the prompts to set and confirm a new password. Keep this password in a secure location, as it cannot be recovered. This password is only for `airsh` physical console access and is not used when you access `airsh` remotely.



CAUTION: If this password is lost, you will need to do a factory reset to clear the password.

Common Commands

help

List available commands. Use `help tree` to see commands and options.

help tree

List available commands with their options. Use `help` to see a list of commands.

setup-ui

Open the setup wizard to set up an Airwall Gateway. See [Configure an Airwall Gateway with the airsh Setup Wizard](#) on page 237.

conf network

v2.2.10 and later – Configure port groups, see [Configure Port Groups with Airshell](#) on page 312.

v2.2.8 and earlier – Set up static IP addresses.

ping

Test network connectivity

status

See Airwall status:

- **Hostname** – Shows the Airwall Gateway's identity used when it connects to the Conductor. You use this name to confirm the provisioning request from the Airwall Gateway.
- **HIT** – The Host Identity Tag is a hash of the Airwall Gateway's Host Identity, the public key identifier. This IPv6-like identifier is used for secure communication.
- **LSI** –The Local Scoped Identifier is a shortened IPv4 version of the HIT, used for secure communication.
- **Device cert.** – Present indicates the presence of a device certificate, which means the Airwall Gateway has been provisioned by the Conductor.
- **Device key** – Present indicates the presence of the device identity private key.
- **Keystore** – Indicates where the device identity private key is stored: TPM, Operating System, or file-based keystore.
- **Annunciator** – Displays the status of the annunciator. On some models this affects LEDs and/or LCD display.
- **Run mode** – Indicates the mode the Airwall Gateway is running in:
 - **Protected** – Normal operation mode.
 - **Transparent** – Running with non-encrypted bridging.
 - **Diagnostic** – In diagnostic mode.
 - **Factory reset** – In factory reset mode.
 - **HA primary/secondary/active** – Indicates the High Availability role of the Airwall Gateway.
- **Conductor** – See status of the connection to the Conductor. For more details, see `status conductor` below.
- **IP address** – Shows the active IP addresses for this Airwall Gateway. An IP address displayed in green indicates it has been selected as active.

status conductor

Shows the status of the Airwall Edge Service's connection to the Conductor. Disconnected indicates the Airwall Edge Service is not connected to the Conductor.



Note: For Airwall Agents and Servers that support it, if Disconnected mode is On, you can still access resources on the Airwall secure network, and your Airwall Agent or Server will reconnect at intervals for configuration and trust policy updates. If you want to reconnect manually, use `conductor sync`.

conductor setSet or remove a Conductor IP address or URL and port (optional). For example: `conductor set my-`

conductor sync	conducto.tempered or just conductor set to remove.
diag	If an Airwall Agent or Server is set to Disconnected mode on the Conductor, this command manually reconnects to retrieve any changes to configuration or trust policies. In Disconnected mode, you can still access resources on the Airwall secure network. See Sync an Airwall Agent or Server in Disconnected Mode on page 29.
factory-reset	Put the Airwall Gateway in diagnostic mode
	Reset Airwall Gateway back to factory default settings. If you want to preserve the network configuration, use the keep-networking option:
	<pre>airsh>> factory-reset keep- networking</pre>
exit or quit	Exit Airshell
history	See the history of commands entered into Airshell. Enter history clear to delete history.
color on off	Turn on or off color on the text output from the serial console.
reboot	Restart the Airwall Gateway.
shutdown	Shut down the Airwall Gateway.

Configuration Commands

activate [activation_code]	Activate a profile, and optionally, enter an activation code to connect an Airwall Gateway to the Conductor. For example:
	<pre>airsh>> activate 8z130f85eed9</pre>
	Entering an activation code means the Airwall Edge Service can connect to the Conductor without an administrator needing to provision it.
conf	Configure Airwall Gateway or Conductor. You can configure these settings
	<ul style="list-style-type: none"> • conf conductor URL IP_address – Set Conductor URL. Same as conductor set above. • conf cell [apn=auto <apn>] [carrier=auto <carrier>] [mode=3g 4g] [pin=<code>] [auth=none pap chap both] [user=<user>] [pw=<password>] [ip-type=<default,ipv4,ipv6,ipv4v6>] [roaming=<0 1>] –Get or set cellular modem configuration – Get or set cellular modem configuration.

- `conf cell2 [apn=auto|<apn>] [carrier=auto|<carrier>] [mode=3g|4g] [pin=<code>] [auth=none|pap|chap|both] [user=<user>] [pw=<password>] [ip-type=<default, ipv4, ipv6, ipv4v6>] [roaming=<0|1>]` – Get or set cellular modem configuration – Get or set second cellular modem configuration.
 - `conf network –`
- v2.2.10 and later** – Configure port groups, see [Configure Port Groups with Airshell](#) on page 312.
- v2.2.8 and earlier** – Set up static IP addresses.
- `conf password [delete]` – Set (or delete) the password for the current Airshell user. Use `conf password delete` to remove the password. (`conf password delete` not available remotely)
 - `conf ssh on|off|status` – Enable, disable, or see the status of remote log in through SSH. See [Set up Remote Access to Airshell](#) on page 310 for full details.
 - `conf ssh-key add ssh_public_key` – Add or remove public SSH keys you use to log in remotely. See [Set up Remote Access to Airshell](#) on page 310 for full details.
 - `conf ssh-key remove` – Remove the public SSH key you use to log in remotely. See [Set up Remote Access to Airshell](#) on page 310 for full details.
 - `conf wifi` – On WiFi-enabled Airwall Gateways, walks you through the steps to configure a WiFi connection.

setup-ui

v2.2.10 and later – Open the setup wizard to set up an Airwall Gateway. See [Configure an Airwall Gateway with the airsh Setup Wizard](#) on page 237.

Diagnostic Commands

conductor status

Show Conductor settings and status.

conductor set

Set or remove a Conductor IP address or URL and port (optional). For example: `conductor set my-conductor.tempered` or just `conductor set` to remove.

diag

Put the Airwall Gateway in diag mode.

diag_report

Get a diagnostic report.

factory-reset [clear-identity]

Reset the Airwall Gateway to factory settings. Use with `clear-identity` to remove the device identity and licensing, and re-licensing the Airwall Gateway.

firmware-upgrade

Update the Airwall firmware from a file hosted on a reachable file server.

network-restart

Restart the network interfaces on the Airwall Gateway.

ping *IP_address* [-I *interface*]

Ping the IP address, optionally with the interface specified with -I.

Status Commands**log [*follow*]**

Show the latest lines of the system log. Use *follow* to follow the log output until you quit with CTRL+C.

status [<option>]

Display the status of the Airwall Gateway, or with an option, display the status of one of the following:

- **conductor** – Get the status of connection to the Conductor
- **linkmanager** – Get Linkmanager status.
- **cell** – Get Cellular information
- **wifi** – Get Wifi information
- **network** – Get Network information
- **macs** – Get the MAC addresses for all of the network interfaces on this Airwall Gateway.
- **routes** – Get routing tables
- **peers** – Get a list of peer Airwall Edge Services
- **ps** – Get the running processes on this Airwall Gateway.
- **tunnels** – Get a list of tunnels on this Airwall Gateway
- **relays** – Get relay probe information
- **hip** – Get HIP state
- **hipvars** – Get additional HIP state

Linux Airwall Server Airshell commands

These are the common Airshell commands for the Linux Airwall Server.

help

List available commands. Use **help tree** to see commands and options.

service [start | stop | restart]

Start, stop, or restart the Linux Airwall Server.

profile [activate | create | list | modify]

Manages profiles for your Linux Airwall Server.

- **activate** – Make a profile the active one. For example: `sudo airsh profile activate <profile name or number>`
- **create** – Create and configure a new profile. For example: `sudo airsh profile create name=<new profile name> conductor=<conductor_url> [act=<activation_code>]`
- **list** – List your profiles. Use `list verbose` to get profile details as well.
- **modify** – Modify a profile. For example `sudo airsh profile modify <name>`

```
number> [name=<new-name>]
[conductor=<conductor-url>]
[act=<activation-code>]
```

conductor [set | sync | status]

- **conductor set** – Set or remove a Conductor IP address or URL and port (optional). For example: `conductor set my-conductor.tempered`. To remove a Conductor, run without a URL: `conductor set`.
- **conductor sync** – If the Airwall Server is set to Disconnected mode on the Conductor, run this command to manually reconnect and retrieve any changes to configuration or trust policies. In Disconnected mode, you can still access resources on the Airwall secure network. See [Sync an Airwall Agent or Server in Disconnected Mode](#) on page 29.
- **conductor status** – Same as `status conductor`, shows the status of the Linux Airwall Server connection to the Conductor.

log follow

status [conductor | wifi | network]

Watch the log file (usually for troubleshooting).

Shows the status of the Linux Airwall Server connection to the Conductor, status of the WiFi connection, or status of the network.



Note: A Conductor status of Disconnected indicates the Linux Airwall Server is not connected to the Conductor. If Disconnected mode is On, you can still access resources on the Airwall secure network, and your agent will reconnect at intervals for configuration and trust policy updates. If you want to reconnect manually, use `conductor sync`.



Note: If your status is Disconnected and Disconnected mode is Off, you will not be able to access resources. Contact your Conductor administrator.

Set up Remote Access to Airshell

You can enable and set up a secure shell (SSH) public key on physical Airwall Gateways to allow you to remotely log in to run `airsh` commands. Remote access is limited to running `airsh` commands, and only to the Overlay IPs, not any Underlay IPs. Remote access uses SSH public/private key pairs, where the Airwall Gateways only see the public key.

Setting up remote access provides a way to configure and troubleshoot your physical hardware without a site visit.



Note: To enable SSH access and add the SSH keys, you first need physical access to the Airwall Gateway.

Before you begin:

To set up remote access, you need:

- SSH public and private keys for the people's computers that require access – For example, these can be generated using OpenSSH's `ssh-keygen` command. For example, `ssh-keygen -t rsa`.



CAUTION: You should protect your SSH private key with a passphrase.

- The Airwall Gateway's Overlay IP address where SSH will be used.
1. If you need to configure an Overlay IP for this Airwall Gateway, you can do it from the Conductor or using Diagnostic Mode on the Airwall Gateway:
 - **From the Conductor:** Open the Airwall Gateway and go to the **Ports** tab. Expand the **Overlay Port Group**, and under **IP addresses**, configure one or more static IP addresses.
 - **From the Diagnostic Mode web interface:** Navigate to `http://192.168.56.3`, open **Settings**, **Port Settings**, and under **Port Groups**, configure an IP address for an Overlay Port Group.
 2. See [Connect to a physical Airwall Gateway or Conductor with a console port](#) on page 246 to connect to the Airwall Gateway and log in to `airsh`.
 3. Enable SSH access by entering:

```
airsh» conf ssh on
```

This enables SSH access via the Overlay IP (not the Underlay IP addresses).

4. Password-based SSH login is not allowed. Configure at least one public SSH key by entering:

```
airsh» conf ssh-key add <public_SSH_key>
```



Note: There is a potential issue on Airwall Gateway 150s v2.2.8 and earlier when copying and pasting long values (over 35 characters) into the console. If the console becomes unresponsive, try pasting the key in smaller parts.

5. In `airsh`, type `status` to get the IP address to log in to.
6. To log in remotely, `ssh` into the IP address, and then log in to `airsh`:

```
login airsh
```

You can now run `airsh` commands remotely on the Airwall Gateway. See [Access an Airwall Gateway Remotely](#) on page 311.

Access an Airwall Gateway Remotely

Once you've [Set up Remote Access to Airshell](#) on page 310 on an Airwall Gateway, you can use the configured SSH key to log in remotely and run a limited set of `airsh` commands with `airsh` as a username.



Note: Remote access is limited to running `airsh` commands, and only to the Overlay IPs, not any Underlay IPs.

For example, if the Overlay IP for the Airwall Gateway is 192.168.50.5, use a command such as:

```
ssh airsh@192.168.50.5
```

You can configure the Overlay IP as a protected device. When policy has been granted to the Overlay IP, you can access remote SSH from a device behind another Airwall Gateway, or from an Airwall Agent.

For full descriptions of `airsh` commands, see [Airwall Gateway Airshell console commands – airsh](#) on page 305.

Configure an Airwall Gateway with the airsh Setup Wizard

Configure the most common Airwall Gateway setup options using the `airsh` Setup Wizard.

Supported Versions

2.2.10 and later Airwall Gateways

Supported on these Airwall Edge Services

All Airwall Gateways

Before you begin

Collect the following information to set up your Airwall Gateway:

- **Underlay network information** – The protocol (DHCP or static) and type (IPv4 or IPv6) of your underlay network, both wired and Wifi, if enabled. If you are using cell, also your APN (for both modems if you have 2).
- **Conductor address** – The IP address or hostname and port for the Airwall Conductor you want this Airwall Gateway to connect to.
- **Wifi information (if enabled)** – The authentication type, SSID and key for your wireless network.
- **Cellular information (if included)** – Your active carrier, preferred access type (3G or 4G), pin code, authentication type (None, PAP, CHAP, PAP/CHAP), username and password (if applicable), IP connection type (default, IPv4, IPv6, IPv4/IPv6) and whether you want to enable or disable roaming.

Set up an Airwall Gateway with the `airsh` Setup Wizard

1. Connect a computer or [Configure an Airwall Gateway with the airsh Setup Wizard](#) on page 237 to access it remotely.
2. Log in to `airsh`. For information on how, see [Airwall Gateway Airshell console commands – airsh](#) on page 305.
3. At the `airsh` prompt, enter:

```
setup-ui
```

4. Fill in the information to set up your Airwall Gateway.
5. When you're finished, the status page shows the options you've selected and whether you are connected to your Wifi or cellular network. You may want to note your underlay IPs.

You can reboot to start using the Airwall Gateway, or go into Diagnostic mode to configure more options.

To troubleshoot connection issues, see [Troubleshoot Initial Airwall Gateway connections](#) on page 415.

Configure Port Groups with Airshell

You can use Airshell to add, delete, and configure port groups on an Airwall Gateway, including adding an Overlay IP.

Supported Versions

2.2.10 and later Airwall Gateways

Supported on these Airwall Edge Services

All Airwall Gateways

Before you begin

By default, port 1 of the Airwall Gateway is an underlay port set to acquire its IP address using DHCP. To configure the underlay port with a static IP address, you'll need:

- IP address/subnet, gateway, and DNS servers for the port group.
- If you are using DHCP, set up your DHCP server on your network.



Note: This procedure uses the `conf net` menus, but you can accomplish the same thing in one command. Enter `help conf net` to see options, and see the one command example after the procedure.

Set up port groups on an Airwall Gateway

1. Connect a computer or [Set up Remote Access to Airshell](#) on page 310 to access it remotely.
2. Log in to Airshell. For information on how, see [Airwall Gateway Airshell console commands – airsh](#) on page 305.
3. At the `airsh>>` prompt, type:
`airsh>> conf network`

Airshell displays the Port Groups configuration menu:

```
Port Groups:
```

```
1: Underlay Port Group 1 [underlay]
  (static) 10.0.1.99/24 gateway: 10.0.1.1 dns: 8.8.8.8
```

```

2 : Overlay Port Group 1 [overlay]

a. Add port group
d. Delete port group
s. Save port group changes
q. Quit (cancel changes)

```



Note: You can also accomplish the same thing in one command. Enter `help conf net` to see options.

- Follow the menus to configure the port groups and port group settings for the Airwall Gateway. Type `q` to back up to the main menu, then type `s` to save your changes.

For more information about editing port groups and port group settings, see [Set up Port Groups on an Airwall Gateway](#) on page 321.

For example, here's how you add an Overlay IP address:

One command line:

```
airsh conf net modify pg="Overlay Port Group 1" ip=[ip_in_CIDR_format]
```

Using the conf net menus:

- At the `airsh>>` prompt, type:

```
airsh>> conf network
```

- Select 2 to edit Overlay Port Group 1.
- Select a to add an Overlay IP group. This adds a static IP address.
- Select 1 (one) to change the static IP address. Airshell displays the IP configuration menu:

```
=====
Configuring IP for Port Group 1
t. Toggle dhcp/static (static)
   i. IP address      (not set)
   g. Gateway         (not set)
   d. DNS Servers    (not set)
q. Quit to previous menu
```

- Select i to enter an IP.
- Enter the IP address you want in CIDR format, and press `Enter`.
- Select q twice to go back to the main menu, and then select s to save the configuration.

Set a Private APN for your Cellular Provider on an Airwall Gateway

You can set the APN of the cell modem on an Airwall Gateway (100, 110, 150, 250) on the Airwall Gateway from Diagnostic mode or using `airsh`, or from the Conductor.



Note: If you are using the default APN of your cellular provider for Internet access, this APN is automatically used when the APN is set to "auto". These instructions are if you have a private APN that you need to set.

Set the APN from Diagnostic Mode

- Put your Airwall Gateway into Diagnostic mode. See your platform guide or [Put an Airwall Gateway into diagnostic mode](#) on page 411 for instructions.
- In **Diagnostic** mode, open the **Settings** page, and the **Port Settings** tab. (*Note: Not the **Cellular Settings** tab.*)
- Select **Edit Settings**.
- For **APN**, enter the APN needed to connect to your cellular service.
- Select **Update Settings**.

Set the APN with airsh

On the Airwall Gateway, you can use the following `airsh` command to set the APN, replacing <APN> with the APN (no spaces allowed):

```
airsh> conf cell apn=<APN>
```

For example,

```
airsh> conf cell apn=my_private_apn
```

For more information on using `airsh`, see [Airwall Gateway Airshell console commands – airsh](#) on page 305.

Set the APN in the Conductor

If the Airwall Gateway is on Ethernet and connected to the Conductor, you can set the APN from the ports page of the Airwall in Conductor.

1. On the page for the Airwall Gateway, open the **Ports** tab.
2. Select **Edit Settings**.
3. Under **Ports**, select the **Cell** Interface.
4. To the right, under **APN**, enter or change to the APN needed to connect to your cellular service.



5. Select **Update Settings**.

Bulk Configuration of Airwall Edge Services

Configure certain settings in bulk for Airwall Edge Services or Airwall groups.

Supported Versions

Conductor 2.2.10 and later

Required Role

System Administrators, and Network administrators with permissions to change the selected Airwall Edge Services

Supported on these Airwall Edge Services

Provisioned and managed

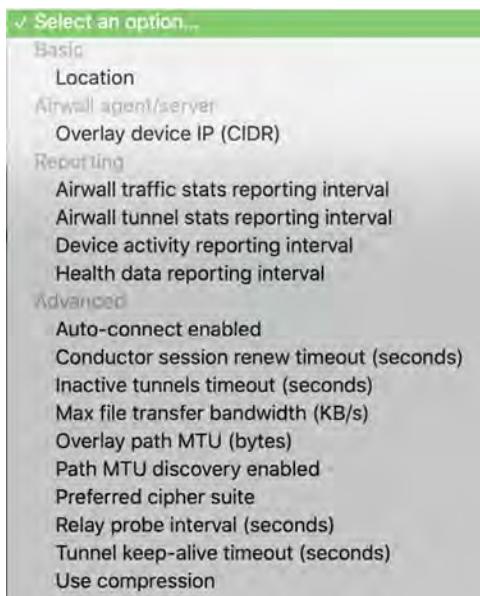


CAUTION: For most options, bulk editing **overwrites** any existing values on the selected Airwall Edge Services. There are a few that you must specifically choose overwrite.

To configure Airwall Gateways in bulk

1. On the **Airwalls** page, select the Airwall Edge Services or Airwall groups you want to configure.
2. Select **Airwall actions > Configure selected Airwalls**.

- Select the options you want to change for all selected Airwall Edge Services. You can select all of the options you want first, and then fill them all in:



- Fill in the values for the options you've chosen.

The dialog box has the following fields:

- Location:** East Coast, with an Overwrite checkbox and a trash icon.
- Overlay device IP (CIDR):** (empty input field), with an Overwrite checkbox and a trash icon.
- Auto-connect enabled:** (empty input field), with an Overwrite checkbox and a trash icon.
- Select an option...:** A dropdown menu.

At the bottom are **Update** and **Cancel** buttons.

- For most options, bulk editing by default overwrites any existing values on the selected Airwall Edge Services. On options that don't automatically overwrite values, you have the option to overwrite. Check **Overwrite** if you want to also overwrite these option values.
- Select **Update** to apply the bulk configuration.

Bulk Edit Settings Descriptions

Here are descriptions for the Airwall Edge Service settings you can configure in bulk.



CAUTION: Most of these options **overwrite** the current setting on selected Airwall Edge Services. A few options (*starred) will not overwrite by default, and instead only apply the change if the setting is blank or has not been changed from the default. For these options, check **Overwrite** to overwrite these option values.



Note: If an option doesn't apply to a particular Airwall Edge Service, it is ignored.

Basic

- Location*** – Physical location of the Airwall Edge Services.

Airwall agent/server

- **Overlay device IP (CIDR)*** – Assign IPs to the selected Airwall Agents and Servers in order from the specified IP CIDR.

Reporting

Set reporting intervals. All of these settings default to 5 minutes:

- **Airwall traffic stats reporting interval** – How often to report traffic stats to the Conductor. Traffic stats are shown on the page for each Airwall Edge Service under **Reporting > Traffic stats**.
- **Airwall tunnel stats reporting interval** – How often to report tunnel stats. Tunnel stats are shown on the page for each Airwall Edge Service under **Reporting > HIP tunnel stats**.
- **Device activity reporting interval** – How often to report device activity.
- **Health data reporting interval** – How often to report health data. Health data is shown on the page for each Airwall Edge Service under **Reporting > Health data**.

Advanced

- **Auto-connect enabled** – Enable to build secure tunnels between devices even if there is no traffic. Useful when devices are behind NAT. **Default:** Enabled
- **Conductor session renew timeout** – Number of seconds before a Conductor session times out. **Default:** 120 seconds.
- **Inactive tunnels timeout** – Number of seconds before an inactive tunnel is closed.
- **Max file transfer bandwidth** – Limit the bandwidth used for large file downloads (such as firmware updates). **Default:** 1000 Kb/second.
- **Overlay path MTU** – Maximum transmission unit (MTU) in bytes sent through the overlay. Must be between 1280 and 9022. **Default:** 1400 bytes.
- **Path MTU discovery enabled** – Check to have the Airwall Edge Service adjust packet sizes if the intermediate routings only support limited maximum transmission unit (MTU) settings. **Default:** Disabled.
- **Preferred cipher suite** – Select the cipher suite to use when encrypting traffic. Default: Use Global setting (set in Conductor Settings under **Advanced > Global Airwall settings**).
- **Relay probe interval** – If enabled, the Airwall Gateway periodically sends probe packets to all of its relays and uses the closest relay when initiating secure tunnels. This option can reduce the amount of network traffic used to build new tunnels and allows auto-connect to be turned off. **Default:** 30 seconds.
- **Tunnel keep-alive timeout** – Enable to have the Airwall send keep-alive packets to peer Airwalls to keep the tunnel from expiring if no device traffic is available. **Default:** 75 seconds.
- **Use compression** – Turn on to have Airwall Edge Services compress encrypted traffic before sending. **Default:** Use Global setting (set in Conductor Settings under **Advanced > Global Airwall settings**).

Set up a secure IPv6 overlay

You may want to set up IPv6 to provide encrypted communication to the IPv6 Internet or between Airwall Gateways, to secure IPv6 communication, and carry IPv6 traffic across an IPv4 only network.

Supported Versions

Conductor and Airwall Gateways 2.2.10 and later
Conductor

Supported Airwall Edge Services

Airwall Gateways v2.2.10 and later, plus any version of Airwall Relay, since they do not decrypt traffic, they will relay IPv6 traffic.

Required Role

System and network administrators with permissions to the Airwall Gateways.



Note: IPv6 is not yet supported on:

- L2 (aka subnet extension) – Having the same subnet behind multiple Airwall Gateways or multiple port groups on a single Airwall Gateway

The steps are:

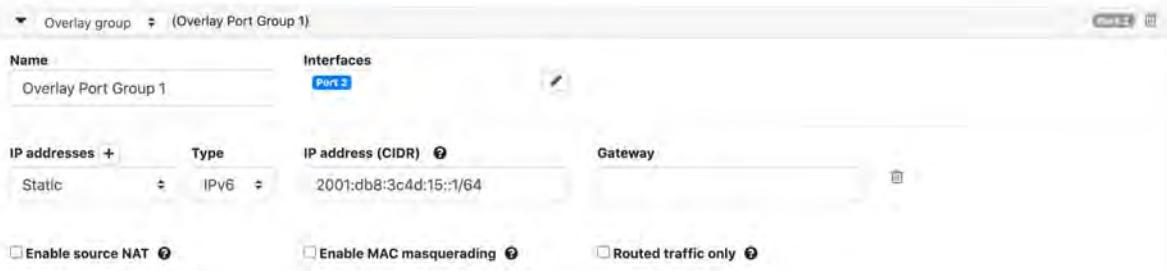
1. Configure an IPv6 static address for an Airwall Gateway
2. Configure DHCPv6 (Optional if you configure a static IPv6 address and a default route to the Airwall's overlay IPv6 address on each IPv6 protected device)
3. Discover devices, or create an /64 network object device on the Airwall Gateway
4. Repeat steps 1-3 for other Airwall Gateways you want to communicate over IPv6.
5. Set up an overlay and add trust between the /64 network object devices.

These steps are covered in more detail in the following sections.

Step 1: Configure an IPv6 static address

On an Airwall Gateway that supports IPv6, add an IPv6 overlay IP address:

1. Go to **Ports**, select **Edit Settings**, and open an Overlay port group.
2. Set the following options:
 - **IP addresses** – Select **Static**. If you need to add an address, click the plus (you can have both IPv4 and IPv6 static addresses assigned).
 - **Type** – Select **IPv6**.
 - **IP address** – Enter a /64 block and assign the overlay IPv6 address (best practice is to use ::1):



Note: Assign unique IP addresses for each Airwall Gateway you set up.

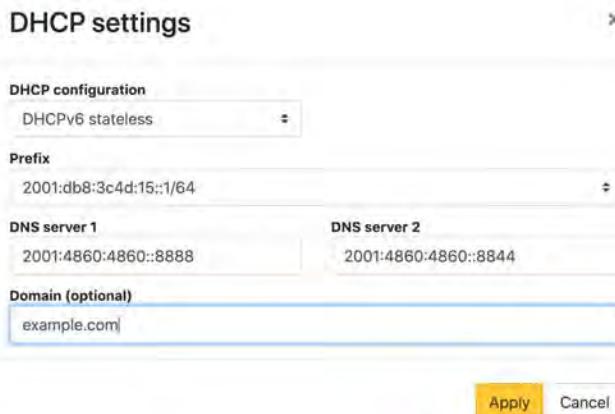
3. Select **Update Settings**.

Step 2: Configure DHCPv6

Note: This step is optional if you configure a static IPv6 address and a default route to the Airwall Gateway's overlay IPv6 address on each IPv6 protected device.

On the Airwall Gateway, configure your DHCP settings for DHCPv6:

1. Next to **DHCP settings**, select **Configure**.
2. Enter your DNS servers and Domain. The rest should be filled in for you.



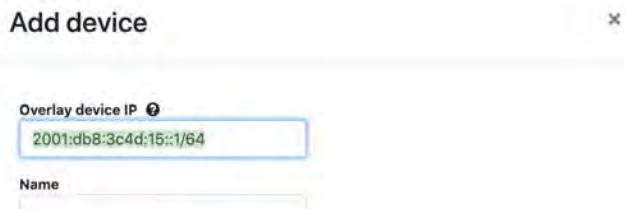
3. Select Apply.

Step 3: Discover devices, or create a /64 network object

You can wait for automatic device discovery to detect IPv6 devices and accept them, or you can create an IPv6 network object if you do not need to set policy for individual devices. If you choose to discover and accept individual IPv6 devices, be aware that the devices may have IPv6 privacy extensions enabled that cause the device to obtain a new IPv6 address frequently (approximately every 15 minutes).

To create a IPv6 network object device on the Airwall Gateway for your local /64 network:

1. Go to **Local devices**.
2. Select **Add device**.
3. Under **Overlay device IP**, enter the static IPv6 IP address you set up on the Overlay port group:



4. Fill in other device details, and then select **Create**.

Step 4: Repeat for one or more Airwall Gateways

Repeat steps 1-3 above for additional Airwall Gateways.

Step 5: Set up trust between IPv6 devices

Add the IPv6 network objects (or discovered IPv6 devices) to an overlay, and set up trust between them. See [Create an overlay network](#) on page 355 and [Add and remove device trust](#) on page 360.

Trust	Device name	Overlay IP	MAC address	OUI	Airwall
None	IPv6 Internet	::/0	F817234E9229		
None	IPv6 Network Object	2001:db8:3c4d:15::/64	110g-South		

Result

IPv6-capable devices connected to these Airwall Gateways can now:

- Obtain an IPv6 address
- Use the Airwall Gateway as their IPv6 default gateway
- Communicate with each other

 **Note:** Some devices may require special configuration to enable IPv6 or IPv6 auto configuration.

Configure an authenticated Airwall Gateway session

An Authenticated Airwall Gateway Session requires users to authenticate before the Airwall Gateway can communicate in an overlay network. The authentication is based on a user's Conductor login credentials.

 **Note:** Authenticated Airwall Gateway sessions expire after 15 minutes of inactivity, or within 24 hours of user log in.

To configure authenticated Airwall Gateway sessions:

1. Go to **Airwalls edge services** and select an Airwall Gateway.
2. Click **Edit Settings**.
3. Check **Require Authenticated Airwall Session**
4. Click **Update Settings**.
5. Point your web browser to a secure (HTTPS) web URL using one of the remote device IP addresses.
6. In the HTTPS login page, enter the Airwall Gateway Conductor username and password.



Note: If the Airwall Gateway is a member of two or more overlay networks, select the overlay networks in which the Airwall Gateway will participate.

Once authenticated, the Airwall Gateway participates in the selected overlay network.



Note: To activate an Airwall Gateway in a different overlay network, you must reboot the Airwall Gateway, re-authenticate, and select the new overlay network.

Configure Advanced Airwall Edge Service Options

Add or Replace a Signed Certificate on an Airwall Gateway for Conductor Communication

By default, the Airwall Gateways come with a Tempered factory-installed certificate. You can add your own custom CA certificate to use for Conductor communication.

Supported Versions

2.2.10 Airwall Gateways and Conductor

Supported on these Airwall Edge Services

Airwall Gateways



Note: When you are in the process of replacing a certificate, the Airwall Gateway uses the existing certificate until the replacement is complete.



Note: For HA-paired Airwall Gateways, you can have a custom certificate on one or both.

Before you Begin

Before you can upload or replace a signed certificate, you need to have a CA certificate chain installed so that the Conductor can verify the certificates. For more information, see [Install a Custom CA Certificate Chain](#) on page 201.

Step 1: Request and copy a CSR (Certificate Signing Request) for the Airwall Gateway

Once you've installed CA certificates (see [Install a Custom CA Certificate Chain](#) on page 201), you can generate a Certificate Signing Request (CSR) to create a certificate (for example, with a PKI Registration Authority) for Airwall Gateway to Conductor Communication:

1. In Conductor, open the Airwall Gateway for which you want to add a custom CA certificate.
2. Go to **Airwall gateway > PKI**.



Note: If the **PKI** tab is not visible, either the Conductor doesn't have custom CA certificate chain uploaded and you need to [Install a Custom CA Certificate Chain](#) on page 201, OR the Airwall version is not 2.2.10 or later.

3. Select Get certificate.

Common name	Purpose	Validity
HS-126.20.91	Conductor communication	04/19/2012-09/24/2040

If you are replacing a certificate, open the **Actions** menu on the existing certificate and select **Replace certificate**.

Certificates

Distinguished Name
/C=US/O=Tempered/OU=Dev/CN=cond.example.com
Ex: /C=US/O=CompanyName/OU=Department/CN=Asset-ID

Request CSR Cancel

- 4.** If you're adding a new certificate, under **Distinguished Name**, enter the Identity (Distinguished Name) for the certificate. For example, `/C=US/O=Tempered/OU=Dev/CN=cond.example.com`

New Conductor communication certificate

Note: If you're replacing a certificate, the Distinguished name remains the same.

5. Select Request CSR.

- 6.** Under **CSR**, select either **Copy** or **Download** to generate and get the CSR you need to get a signed certificate.
7. Select **Cancel** to close the dialog, or leave it up while you get the signed certificate.

Step 2: Get a signed certificate

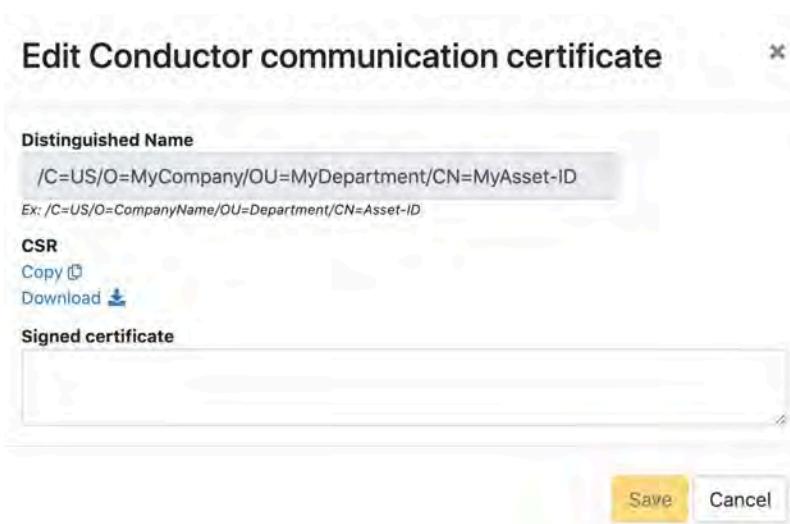
Use the CSR to request a new signed certificate. You can generate a new signed certificate using your organization's own process, or with a public PKI Registration Authority.

1. Submit the Certificate Signing Request (CSR) you copied or downloaded to your Enterprise PKI Registration Authority. They use it to create your certificates.
2. When you get the certificates, download or copy them.

Step 3: Upload the signed certificate to the Airwall Gateway

1. In Conductor, open the Airwall Gateway for which you have a custom CA certificate.
2. Go to **Airwall gateway > PKI**.
3. Open the **Actions** menu on the existing certificate and select **Edit**

- Under **Signed Certificate**, paste the custom-CA signed certificate to install the certificate on the Airwall Gateway.



- Select Save.

Set up Port Groups on an Airwall Gateway

The default port groups work for some deployments. You may need to set up underlay or overlay port groups if your deployment requires it.

Set up Overlay Port Groups

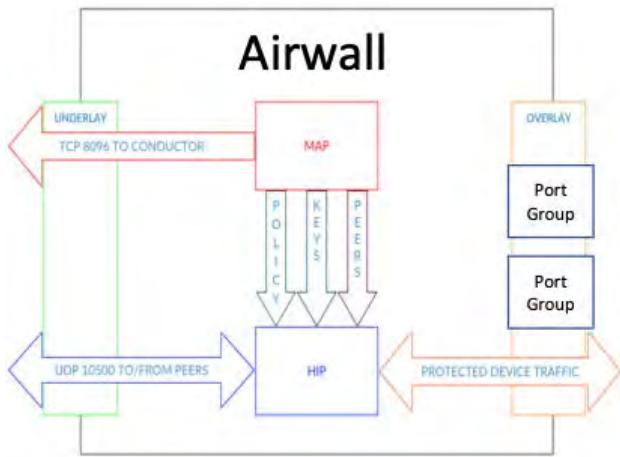
The default port groups work for some deployments. You may need to set up overlay port groups if your deployment requires it.

Overlay Port Groups are used to connect your Airwall Gateway to your protected networks. Airwall Gateways default to having a single overlay Port Group, but you may need to configure your overlay port groups when you want to:

- Micro-segment your network for fine grain security control
- Configure IP addresses or Source NAT (SNAT) for routed deployments
- Set up two Airwall Gateways for High Availability

If your Airwall Gateway is only providing relay functionality, it only needs an Underlay Port Group, and doesn't use any configured Overlay port group.

You can set up multiple port groups for an overlay, assigned to different physical or VLAN tagged sub-interface ports. When multiple ports are included in a Port Group, they are bridged. Port groups are also connected to the overlay through routing and/or bridging.



Get to Know Your Airwall Gateway Ports

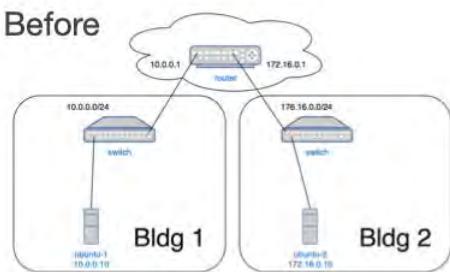
Here's how the physical ports are assigned on most Airwall Gateways:

- Port 1 – Connects to the initial underlay network, and is assigned to the underlay Port Group.
- Port 2 & Up – Connect to overlay networks, and are assigned to an overlay Port Group.

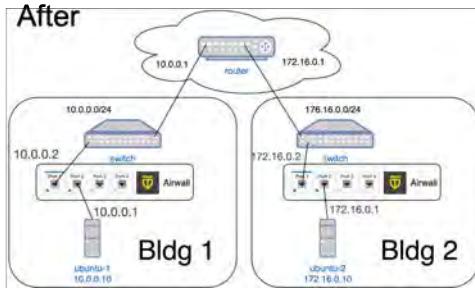


Basic Airwall Gateway Deployment

The most basic Airwall Gateway deployment design is to put Airwall Gateways inline in front of protected devices. If you don't want to, or can't, change IP addresses, you replicate the default gateway of the router on the overlay Port Group. (If these devices are using DHCP, see [Protected devices with static routing](#) on page 346 to configure DHCP on the overlay port group.)



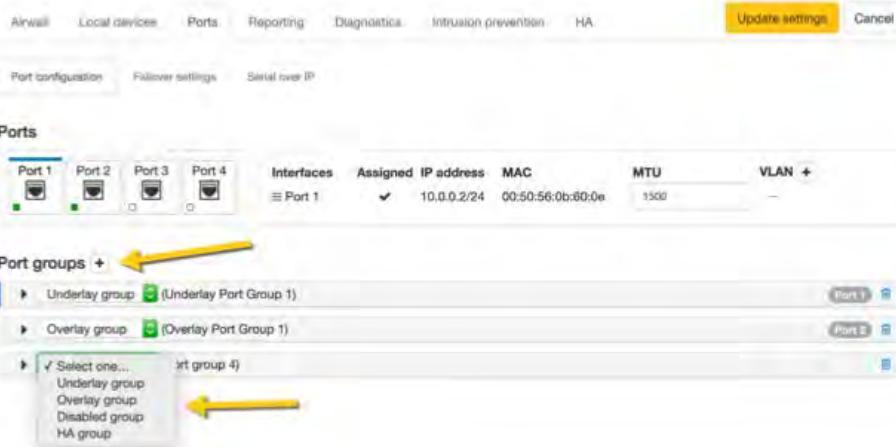
The underlay IP address can be any address on the network. DHCP is common, or you can configure a static IP if needed. The overlay IP address is the same as the default gateway on the router.



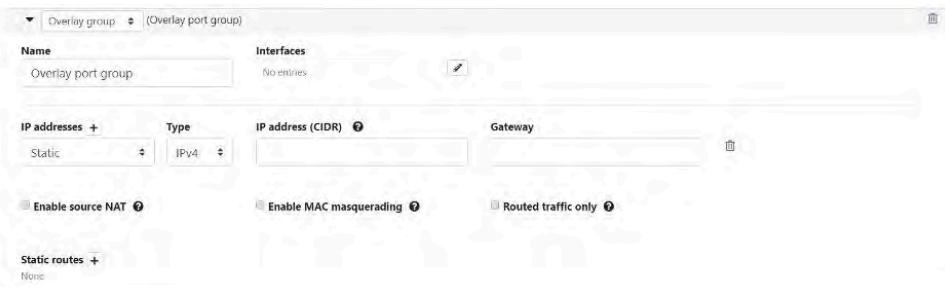
Set up an Overlay Port Group

By default, an Airwall Gateway has two port groups. One underlay port group assigned to Port 1 and one overlay port group assigned to the remaining ports. On virtual and cloud Airwall Gateways, you may be able to configure more ports if supported by the virtual or cloud platform.

1. In the Conductor, go to the Airwall Gateway on which you want to set Port Groups, open the **Ports** tab, and select **Edit Settings**.
2. Select an Overlay port group you want to use, or add a new port group by clicking the + to the right of **Port groups**, and select **Overlay group**.



3. Click the arrow on the left of your **Overlay group** header to expand the settings for that Port Group.



4. Enter a name for the group, and under **Interfaces**, select the ports or other interfaces for the group.
5. Under **IP addresses**, click the + to add IP addresses. For example, 10.0.1.1/24 (be sure to include the prefix length). Your protected devices will use this address as their gateway to reach the rest of your overlay network.
6. Select the network options that apply for your implementation:
 - a) **Enable Source NAT** – Check this box to rewrite the source IP address of traffic arriving from other port groups or tunnels with the overlay IP address of this port group. You must also configure an overlay IP address. Use this option when your local protected devices do not use this Airwall Gateway as their default gateway. This setting enables connections, permitted by policy, from remote overlay devices to local protected

devices. When you enable Source NAT, local protected devices cannot initiate connections to remote overlay devices.

- b) **Enable MAC masquerading** – Check this box to rewrite the source MAC address of all traffic arriving from other port groups or tunnels with the Airwall's MAC address. Use this option if the network you are connected to doesn't permit foreign MAC addresses. Note: Checking the Routed traffic only box enables MAC masquerading by default.
- c) **Enable spanning tree protocol** – Leave this box checked to enable spanning tree protocol on the overlay bridge to avoid potential bridge loops. Only clear this box if this port group is free of any bridge loops, and you do not wish to run STP. One example is if this port group is connected to a Cisco switch running BPDU guard. A recommended alternative is to configure the port group with only a single port and use routed traffic only mode to make bridge loops impossible.
- d) **Routed traffic only** – Check this box to permit only routed bypass traffic. You must also configure an overlay IP address. Local protected devices should use this overlay IP as a gateway (either their default gateway or a static route) or Source NAT to allow incoming connections. Typically, you check Routed traffic only, unless you specifically need to bridge traffic. For example, if you have IP addresses in the same subnet on both sides of the tunnel, you are bridging traffic, so clear this box.

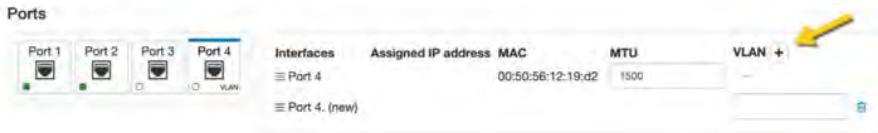
This setting prevents inadvertently carrying broadcast and multicast traffic sent by protected devices and can improve performance by using only a single port in the port group.

7. If you are connecting this port group to a router connected to a larger overlay network, you can configure static routes or even a default gateway.
8. Select **Update Settings**.

Add Interfaces to a Port

Each physical or logical port on an Airwall Gateway has a single interface by default, that can be assigned to a port group. If you are connecting an Airwall Gateway port to a switch using an 802.1q trunk allowing multiple VLANs, you need to add additional interfaces. To do this:

1. Up above the **Port Groups** section, select the **Port** and then click **Edit Settings**.
2. Next to **VLAN**, click the **+** to add a new VLAN for this overlay.
3. Enter the VLAN tag to match the VLAN config on the switch.



Do I need a gateway?

You only need a gateway if the Airwall Gateway needs to know how to reach additional networks from this port. The Airwall Gateway is the gateway for its protected devices. In general, using static routes (for example, 10.0.0.0/8) for your corporate network is preferable to using a default gateway (which is a 0.0.0.0/0 route), particularly if you have a bypass destination of 0.0.0.0/0 set up, since that will cause a conflict.

Set up an Underlay Port Group

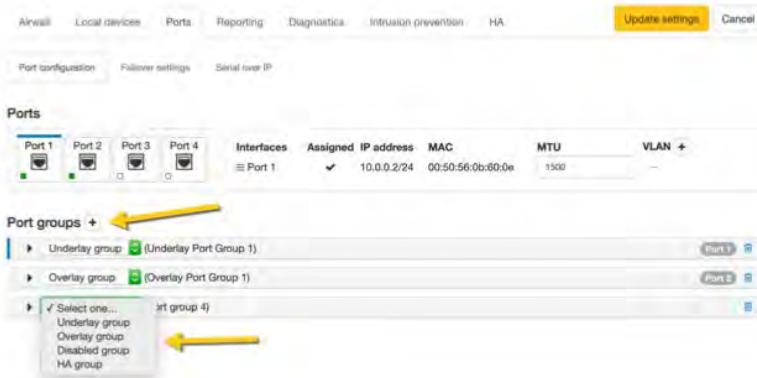
By default, an Airwall Gateway has two port groups. One underlay port group assigned to Port 1 and one overlay port group assigned to the remaining ports. On virtual and cloud Airwall Gateways, you may be able to add additional ports by creating new virtual network adapters on the hypervisor. Some hardware models allow you to add new ports by inserting port expansion modules.

All non-cellular ports allow adding VLAN sub interfaces.

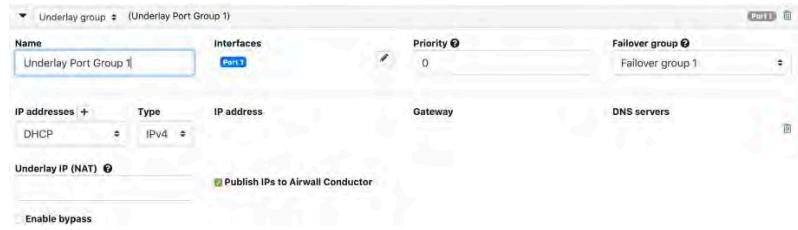
You may want multiple underlay port groups on wireless Airwall Gateways. You can configure one port group for the wireless port and one for a wired port and assign different priorities to the two port groups. This allows the Airwall Gateway to automatically fail over to whichever port is available based on the assigned priorities.

It can also be useful to have multiple wired underlay port groups to allow an Airwall Gateway to communicate on separate networks at the same time. For example on a relay Airwall Gateway, you could configure one underlay port group on a DMZ and the other on the corporate network (multi-homing).

1. In the Conductor, go to the Airwall Gateway on which you want to configure port groups, open the **Ports** tab, and select **Edit Settings**.
2. Select an Underlay port group you want to use, or add a new port group by clicking the + to the right of Port groups, and select Underlay group.



3. Click the arrow on the left of your Underlay group header to expand the settings for that Port Group.



4. Enter a name for the group, and under **Interfaces**, select the port interfaces for the group.
5. Under **Priority**, set the priority for this underlay port group. 0 is the highest priority. The Airwall Gateway will always try to use the underlay port with the lowest priority value if the network is available.
6. (Optional) Under **Failover group**, select the Failover group. Failover groups allow traffic monitoring for a given traffic type (Conductor traffic or data plane traffic). The failover groups define how to monitor the availability of the port groups contained in the failover group, and when port groups should fail over to another port group. Only a single port group is used at a time. Failover groups are configured separately on the **Failover settings** tab.

You can select **Stand-alone** to make the port group permanently available independent of any other underlay port group.

7. Under **IP addresses**, click the + to add an IP address. You can choose between DHCP or static address configuration. The **Underlay Port Group IP address** may be already configured if you configured its initial IP address when setting up the Airwall Gateway.
8. Under **Underlay IP (NAT)**, If this Airwall has a public IP, you can add it here. Remote Airwall Edge Services will then attempt to connect to the public IP instead of the IP configured on the underlay port group.
9. Check **Publish IPs to Airwall Conductor** to advertise the IP address of this underlay port group to remote Airwall Edge Services to build secure tunnels. In a hub and spoke Airwall deployment you may want to leave this unchecked on the spoke Airwall Gateways if tunnels are always established from the spoke to the hub. This configuration reduces network traffic related to IP address advertising.
10. Check **Enable bypass** to allow traffic from protected devices behind this Airwall Gateway to reach destinations on the underlay network. Traffic to these destinations can be configured just like normal overlay traffic using the policy editor. You can configure bypass destinations on the **Devices** tab. Clear this box to disable bypass traffic over this underlay. You can only enable bypass on a single underlay port group on each Airwall Gateway.
11. If you have enabled bypass, you can choose to **Enable source NAT**. This option replaces the source IP of packets leaving the Airwall Gateway with the IP of the port group, and may be required to allow routing between the IP addresses on the device network and the bypass destinations.
12. If your network requires it, you can add additional static routes as needed.
13. Select **Update Settings**.

Replicate Port Settings

For minimal disruption and less room for error, you can replicate the port configuration between two Airwall Gateways when setting up an Airwall Gateway HA pairing, or when replacing an Airwall Gateway.

Follow these links for more information on how it works in each situation:

- [Configure High Availability Airwall Gateways \(v2.2.8 and later\)](#) on page 337
- [Replace an Airwall Gateway](#) on page 111

Configure an Underlay Port Failover Group

Starting in v2.2.8, a failover group is created and set by default. For earlier and updated Airwalls, you may need to create and set it yourself.

1. On an Airwall Gateway, go to **Ports > Failover settings**.
2. Next to **Failover Groups**, click the plus sign (+) to create a new Failover group.
3. Name your group, and if needed, change the default settings for the Failover group.
4. Go to **Ports > Port configuration**, and select **Edit Settings**.
5. Under **Failover group**, select the new group you created.
6. Select **Update Settings**.

Best Practices for Underlay Port Failover Groups

Set your Underlay failover settings to a Failover group as a best practice.

Find your version below for guidelines, and for detailed instructions, see [Configure an Underlay Port Failover Group](#) on page 326.

Best Practice for v2.2.1 to v2.2.5

In v2.2.1 to v2.2.5, Underlay failover settings are set to **Stand-alone** by default. Create a Failover Group and then change the Port Group failover setting from **Stand-alone** to the new Failover Group you created. See [Configure an Underlay Port Failover Group](#) on page 326.

Best Practice for v2.2.8 and later

In v2.2.8 and later, Underlay failover settings are set to an auto-created failover group, “Failover Group 1,” by default. You can create additional groups or edit the default group settings to adjust failover behavior for your Underlay port groups. **Stand-alone** is still available, but it is deprecated and not recommended. See [Configure an Underlay Port Failover Group](#) on page 326.

Manage Failover between Underlay Port Groups

Set up your Airwall Gateways with multiple wired and wireless underlay port groups and configure which port group to use based on simple network criteria.

Supported roles

- System Administrator
- Network administrator with permissions to edit Airwall settings

Managing the Active Network with Failover Groups

You can assign one or more failover groups to underlay port groups on an Airwall Gateway. Failover groups continuously monitor health indicators on the networks of their assigned port groups and manage which one is active based on both the current network health indicators and a relative priority assigned to each port group within the failover group.

The health criteria that a failover group monitors on the network are:

- **Wired interface link status** – If the failover group detects that a port is missing a link, or the layer 3 configuration is bad (for example, has no IP address), the port group is considered failed and is not selected.
- **Cellular modem status** – If there are error conditions on the cellular modem, the failover group sets the corresponding cellular port group as failed.

- **Active monitoring of selected destinations** – You can specify destinations to have the failover group actively check if they are responding. It will ping these destinations and monitor their response. If the pings are successful, the corresponding underlay port group is considered functional. See **Ping Settings** below.
- **Passive monitoring** – The Airwall Gateway uses the currently active Conductor connection as a secondary indicator to determine network health if no active monitor is running.

Based on these monitoring criteria, the failover group scores each assigned port group and selects the one with the highest score. If more than one port group gets the highest score, the failover group selects the port group that has the highest priority.

Set Failover group settings for the Airwall Gateway

1. Go to **Airwalls** and select an Airwall Gateway.
2. Go to **Ports > Failover settings**.
3. Under **Failover settings**, set the common settings to be used by all port failover groups on the Airwall Gateway:



- **Reboot if no links are available** – Enable to reboot the Airwall Gateway if none of the failover groups have any healthy networks, in an attempt to restore the network. The following additional settings also apply to the reboot:
 - **Min. wait time after failure** – Specify how many seconds to wait after detecting that all **port groups** have failed before rebooting. **Default:** 600 seconds
 - **Min. wait time after reboot** – Specify how many seconds to wait before the next reboot if the network remains unavailable after a reboot. Set this to a higher value than the initial wait time to prevent constant reboot loops if the network is unavailable for extended time periods. **Default:** 1800 seconds
- **Enable cellular link auto-repair** – Enable on cellular Airwall Gateways only to attempt to restore a failed cellular modem after detecting that the cellular network is not responding (by re-initializing the modem drivers).

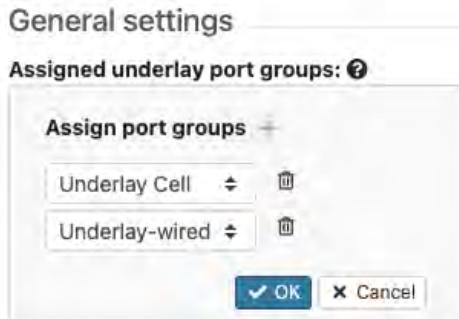


Note: For these settings to take effect, you need to set up at least one failover group on this Airwall Gateway.

Create a Port Failover Group

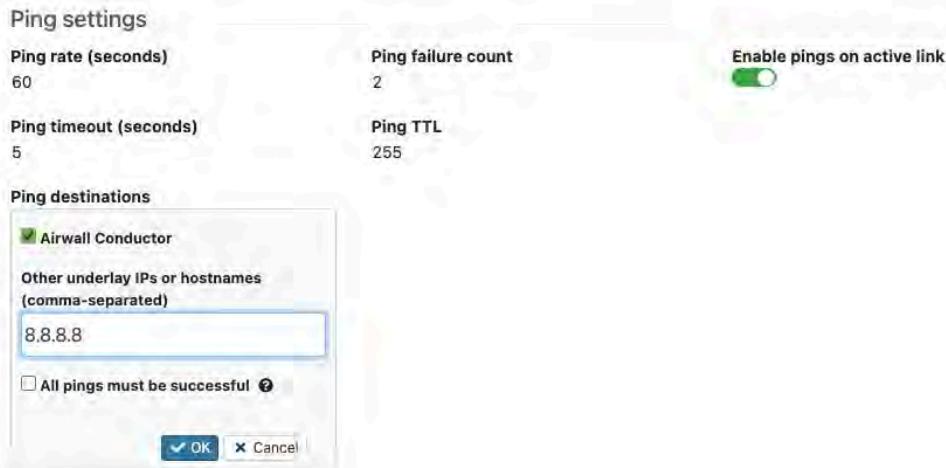
1. Under **Failover group**, select the + (plus sign) to create a new failover group. The Conductor creates a new failover group with default values. You can click on the name to edit it.

2. Under **General settings > Assigned underlay port group**, assign underlay port groups to this failover group:



- a) Click on this setting to edit it.
 - b) Next to **Assign port groups**, select the + (plus sign) to add one of the unassigned underlay port groups to this failover group.
 - c) Select the arrows to choose a different port group, and arrange them from top to bottom in priority order.
 - d) Select **OK** to save your settings.
3. Still under **General settings**, select the traffic types:
- a) **Allowed traffic types** – Click on this setting to edit it. Select one or more underlay traffic types for the failover group to manage. Select **OK** to save:
 - **HIP** – Encrypted overlay traffic between Airwall peers
 - **Conductor** – TLS-encrypted traffic between the Airwall Gateway and the Conductor
 - **Bypass** – Bypass traffic leaving the overlay to the underlay. Selecting Bypass is only useful if you have set up at least one bypass port group on the Airwall Gateway.
 - b) Select **OK** to save your settings.

- Under **Ping settings**, configure any destinations you want to ping to actively monitor the network, along with the ping settings.



- Ping rate** – Set the rate at which the failover group sends out pings, in seconds.
- Ping failure count** – The number of successive ping failures required to consider the ping monitor failed. If the pings are unreliable, you can set a higher number to help stabilize the network selection.
- Enable pings on active link** – Disable to suspend pings for the port group that is currently active. The failover group then does only passive monitoring to detect status changes on the port group.
- Ping timeout** – The time to wait for ping replies before setting the ping as failed, in seconds.
- Ping TTL** – The time-to-live counter. You usually do not need to change this setting. If you want to speed up the time to failure and know the maximum number of hops to the ping destination, you can set the **Ping TTL** to a lower value.
- Ping destinations** –
 - Check **Airwall Conductor** to ping the Conductor configured on this Airwall Gateway. Note that checking this option includes any additional Conductors configured on the Airwall Gateway as well as the High-availability (HA)-peer Conductor if Conductor HA is configured.
 - Other underlay IPs or hostnames** – Add any IP addresses and hostnames to ping, separating them with commas.
 - All pings must be successful** – Leave this box clear so that only a single ping to any of the IPs must be successful for the ping monitor to be successful (recommended). Check to require that all specified IPs and hostnames must respond to be considered successful.

- Select **OK** to save your settings.

Managed and unmanaged port groups

By default, when you first create an underlay port group, it is unmanaged, meaning it won't be automatically assigned to any failover group. If a port group is unmanaged, the Airwall Gateway does not monitor health indicators and won't fail over. The Conductor may still use unmanaged ports for any type of traffic, but if an unmanaged port fails, the Airwall Gateway relies on the underlay networking to recover.

Cellular Airwall Gateways automatically create and assign a failover group when initialized or factory reset. This failover group is configured with cellular and wired ports, and assigns the wired port a higher priority than the cellular. Wired-only Airwall Gateways do not create a default failover group and any wired port groups are left unmanaged.

Seamless Bypass

Seamless Bypass allows you to separate traffic (split tunnel) going through your Airwall Gateway, where you selectively encrypt and tunnel some traffic, while allowing other traffic to pass through the Airwall Gateway unchanged. This ability also allows protected devices to securely communicate with devices or network locations that are not protected by Airwall Edge Services.

For example, you may have devices that need to communicate with software update servers on the Internet. You can configure the software update servers as a bypass destination and establish trust between the bypass destination and the protected devices. This gives the devices the ability to communicate with the bypass destination, while requiring all other access to be through encrypted tunnels from other Airwall Gateways.

This configuration of Seamless Bypass permits traffic between the secure overlay network, and an insecure underlay network, where the Airwall Gateway acts similarly to an SNAT (Source Network Address Translation) gateway. Connections initiated from the underlay network are still blocked, but connections initiated from a protected device to a permitted bypass destination are allowed.

You set up a bypass destination to:

- Permit traffic to exit your secure overlay to destinations not protected by an Airwall Edge Service
- During migration as an intermediate step to protecting all your traffic with Airwall Edge Services
- To allow local devices to continue to access a protected device

Supported Versions

Versions

- Conductor: 2.2.8 and later
- Airwall Gateways: 2.2.8 hardware and virtual gateways, and cloud gateways with some restrictions.

Requirements and Prerequisites

Requirements

- Any other network traffic that you want to send to remote Airwall Gateways supports being routed between subnets, and does not include broadcast or multicast protocols.
- Devices protected by the Airwall Gateway either use DHCP, or can be reconfigured to use the new subnet.

What type of devices can be bypass destinations?

You can set many types of network destinations as bypass destinations. For example:

- Active Directory Servers
- Software Update Servers
- Equipment control systems, such as for HVAC installations.
- The internet, to bypass to everything on the internet.

Before you begin

Before you begin, you need to:

- Have the IP address or hostname of the device or destination for which you want to create a seamless bypass.
- Update your Conductor and the Airwall Gateway to which you want to add the bypass destination to version 2.2.8.
- If you are using a v2.2.10 or later Conductor, and need or want to use a fully qualified domain name (FQDN) instead of IP for your bypass destination, you need to enable bypass DNS. See [Enable DNS lookup for bypass destinations](#) on page 336.

Set up a bypass destination (seamless bypass)

To set up a bypass destination, you need to:

1. Enable bypass on the Underlay Port
2. Set up an Overlay port for the bypass
3. Add protected devices
4. Create a bypass destination
5. Set trust between the bypass destination and protected devices.

These steps are described in more detail in the following sections.

Step 1: Enable bypass on your underlay port on the Airwall Gateway

Set up a bypass port on the Airwall Gateway that is protecting devices that need access to the bypass destination.

1. On the **Airwalls** page, on the **Ports** tab, go to the Underlay Port group, and select **Edit Settings**.
2. Check **Enable bypass**.
3. If you are setting up an L3 or combined L2 and L3 bypass (recommended), also check **Enable source NAT** and **Routed traffic only**.
4. Select **Update Settings**.

Step 2: Set up an Overlay Port group for the bypass

1. On the Overlay Port group, select **Edit Settings**.

2. Check **Routed traffic only**.



Note: Checking this option prevents broadcast and local multicast traffic across this port group. Clear this box to use the same subnet on overlay and underlay sides of this Airwall Gateway.

3. Find an unused subnet and set up a static IP address for the Overlay Port group. Pick a subnet that is not used elsewhere in your network, for example: 192.168.1.0/24. One common convention is to use the first usable IP in the new subnet.
4. Select **Update Settings**.

5. Under **DHCP settings**, click **Configure**.

Overlay group Overlay Port Group 1			
Name	Interfaces		
Overlay Port Group 1	Port 1		
IP addresses	Type	IP address (CIDR)	Gateway
Static	IPv4	192.168.120.1/32	
Enable source NAT	?	Enable MAC masquerading	Routed traffic only
No	?	?	✓
No DHCP settings Configure v4...			
Static routes None			

6. Set up a DHCP server on the overlay so devices connecting to the Airwall Gateway automatically get an IP address:
 - a) Under **DHCP configuration**, select **DHCP server**.

DHCP settings

DHCP configuration

Overlay device IP start: 192.168.1.100 Overlay device IP end: 192.168.1.199

Netmask: 255.255.255.0 Gateway (optional): 192.168.1.1

DNS server 1: 8.8.8.8 DNS server 2: 8.8.8.4

Domain (optional): Lease time: 1h

Apply **Cancel**

- b) For **Overlay device IP start** and **Overlay device IP end**, enter a DHCP range for the devices. For example, 192.168.1.100-192.168.1.199.
- c) **Netmask** - Set to the netmask for the subnet you selected, for example, 255.255.255.0 for the /24 used in this example.
- d) **Gateway** – Set to the Airwall Gateway's overlay IP (192.168.1.1 in this example).
- e) **DNS servers** – Set to your preferred DNS servers. For example, Google's DNS servers at 8.8.8.8 and 8.8.8.4.
- f) Select **Apply**.

For more information, see [Protected devices with DHCP](#) on page 347.

Step 3: Add protected devices and/or a device group, if needed

For details, see [Add devices to the Conductor](#) on page 351.

Step 4: Create a bypass destination



Note: The bypass destination can be shared between all Airwall Gateways on the Conductor that support bypass and have bypass enabled, so if you've already set up a bypass destination, you can skip this step.

1. On the Conductor **Devices** page, on the **Devices** tab, click **Add bypass destination**.
2. Enter the bypass destination:
 - Under **IP address**, enter the IP for the destination of the seamless bypass device. For example, to create a bypass destination for the Internet, enter 0.0.0.0/0.
 - Or, if you have enabled DNS for bypass destinations (v2.2.10 or later), under **Hostname**, enter a fully-qualified domain name (FQDN) instead of an IP address. For example, google.com. For more information, see [Enable DNS lookup for bypass destinations](#) on page 336.
3. Ignore the MAC options.
4. *Optional.* Add a description and tags to help identify the bypass destination.
5. Click **Create**.

Step 5: Set trust between the bypass destination and protected devices

Add the bypass destination and devices or device groups that need to access it to a new or existing overlay, and assign trust between them as you normally would. For more details, see [Create an overlay network](#) on page 355 and [Add and remove device trust](#) on page 360.



Note: You can also set up trust between the bypass destination and individual devices.

You should now be able to plug devices into your Airwall Gateway, and they will be able to get an IP address and connect to the bypass destination.

To see or change settings for your bypass destination

If you need to review or change settings for your bypass destination, you can open it from the **Devices** page.

1. On the **Devices** page, on the **Devices** tab, open **Show all devices** and then select **Bypass destinations**.
2. On the line for your bypass destination, open the drop-down on the right, and select **Edit Properties**. On this page, you can:
 - See or change properties
 - See the bypass destination's membership in Overlays
 - See the remote devices or locations it trusts

Backhaul Bypass

Set up backhaul bypass to allow any v3.0 or later Airwall Gateway to reach bypass destinations by tunneling traffic using designated bypass egress Airwall Gateways.

Supported Roles

- System Administrators
- Network Administrators with the “Can view and edit bypass destinations” permission

Supported Versions

Airwall Gateways and Conductor v3.0 and later. The Airwall Gateways for both ends of the backhaul bypass and your Conductor must all be on v3.0.

Supported Airwall Gateways

All v3.0 and later Airwall Gateways

Only the bypass egress gateways need to enable bypass on an underlay port group and ensure the bypass destination is reachable from this port group.

Any bypass-enabled v3.0 or later Airwall Gateway can be designated as a bypass egress Airwall Gateway and then can be assigned to other Airwall Gateways to use when tunneling bypass traffic. You can also assign a default backhaul Airwall Gateway to use if you haven't specified one to use.

The Conductor determines the bypass gateway to use in this order:

1. Use a local bypass if the Airwall Gateway has a local bypass-enabled port group.
2. Use an assigned bypass Airwall Gateway, if set.
3. Use the Conductor default gateway, if set. The default is used for all v3.0 Airwall Gateways without a local bypass port and with trust set up to the bypass destination on an overlay.



Note:

- Backhaul bypass can be used for any bypass destination including destinations using hostnames.
- Backhaul bypass can use relays just like normal overlay traffic. There is no special configuration needed on the Airwall Relay.
- You can set up backhaul Airwall Gateways with multiple bypass-enabled underlay port groups and use link manager to fail over between them.

Requirements and Considerations

- You must configure at least one underlay port group with bypass enabled on all backhaul bypass Airwall Gateways.
- It is a best practice to enable source NAT (SNAT) and routed-only mode on the bypass port group.
- When using hostname bypass destinations, you must meet these requirements:
 - The DNS server used by the overlay device must be on the Conductor-configured allow-list for bypass DNS.
 - The traffic path to resolve hosts must follow the same path on the overlay as the traffic to the actual bypass destination. This means that the DNS server must itself be a bypass destination and the overlay devices using it must have policy to it.

Set up Backhaul Bypass

1. Set up one or more Airwall Gateways with Seamless bypass, including creating bypass destinations, creating an overlay with devices and the bypass destination, and adding trust. For details, see [Seamless Bypass](#) on page 329.

 **Note:** Bypass destinations are not assigned to individual Airwall Gateways. Any bypass gateway can bypass to any bypass destination, assuming underlay routing and trust is set up.

2. Configure any Seamless bypass Airwall Gateways to be used as bypass Airwall Gateways.
3. (Optional) Set up a bypass Airwall Gateway to be the default for your Airwall secure network. The default is used for all v3.0 Airwall Gateways that don't have a local bypass set up and do have trust set up to the bypass destination on an overlay. (See the Add trust step that follows)
4. Set up other v3.0 Airwall Gateways to use a bypass Airwall Gateways, selecting a specific one to use, or allowing it to use the default. Note that you can assign a bypass gateway using [Bulk Configuration of Airwall Edge Services](#) on page 314.

 **Note:** If you didn't set a default in Conductor Settings, you need to select one to use.

5. Add trust between devices and the bypass destination. For details, see [Add and remove device trust](#) on page 360.
6. (Optional) Set up allowed DNS servers to enable hostname bypass destination. This should already be done when you set up Seamless Bypass. (For instructions, see [Enable DNS lookup for bypass destinations](#) on page 336.)

See the following sections for details on steps 2 through 4.

Configure an Airwall Gateway as a Bypass gateway

Configuring an Airwall Gateway as a bypass gateway allows other Airwall Gateways to use it to access bypass destinations.

1. Go to **Airwalls** and open an Airwall Gateway.
2. Go to the **Ports** tab and select **Edit Settings**.
3. Open any **Underlay port group**, and check **Enable bypass**.

 **Note:** Using routed-only mode and source-NAT is recommended but not required.



The screenshot shows the 'Port groups' configuration screen. An 'Underlay group' is selected, showing 'Underlay Port Group 1'. The 'Interfaces' section lists 'Port 1'. The 'Priority' is set to 0, and the 'Failover groups' are 'Unmanaged'. In the 'IP addresses' section, 'DHCP' is selected for Type, and 'IP address (CIDR)' is listed as 'Underlay IP (NAT)'. There are checkboxes for 'Publish IPs to Conductor', 'Enable bypass' (which is checked), 'Enable source NAT', and 'Routed traffic only'. A 'Static routes' section at the bottom indicates 'None'.

4. Go to the **Airwall gateway** tab and select **Edit Settings**.

5. Under **Advanced settings**, check **Allow Airwall to act as a bypass gateway**, and select **Update Settings**.

Advanced settings

Network communication enabled

Preferred cipher suite: Global default (AES256_GCM) **Use compression**: Global default (Off)

Enable auto-connect

Inactive tunnel timeout: 600 seconds

Conductor session renew: 120 seconds

Enable relay probes

Send probes every: 30 seconds

Send keep-alive

Keep-alive timeout: 75 seconds

Allow Airwall gateway to act as an Airwall relay

Allow Airwall to act as a bypass gateway

Enable path MTU discovery

Enable overlay path MTU

Limit bandwidth for file transfers



Note: If you want to use FQDNs for your DNS servers, check that the DNS resolver has access through the same tunnel as backhaul bypass. For example, backhaul to your corporate office and use the DNS resolver there. This access allows the egress gateway to learn the DNS FQDNs. Also, note that some common DNS over HTTPs (DoH) or DNS over TLS (DoT) settings (for example, on Google Chrome) can prevent hostname based policies from working.

(Optional) Select a default Bypass Airwall Gateway

Select a default Bypass Airwall Gateway for other Airwall Gateways to use so you don't need to specify it for each Airwall Gateway.



Note: The default is used for all v3.0 Airwall Gateways without a local bypass port and with trust set up to the bypass destination on an overlay.

1. In the Conductor, go to **Settings > Advanced > Bypass Settings** and select **Edit Settings**.
2. Under **Default bypass egress gateway**, select the bypass Airwall Gateway you want to use as the default for your Airwall secure network:

Bypass settings

Default bypass egress gateway: None

Enable bypass DNS lookup

Allow Airwall DNS servers

Allowed DNS server IPs (comma-separated list of DNS server IPs): 9.9.9.9,8.8.8.8,208.67.222.22

Minimum TTL: 10 minutes

Update **Cancel**

3. Select Update.

All v3.0 Airwall Edge Services now will automatically use the default as needed, unless you've set them to use a specific one.

Select a Specific Bypass Airwall Gateway

Once you've got a bypass Airwall Gateway set up, you can set up other Airwall Gateways to use it for bypass.

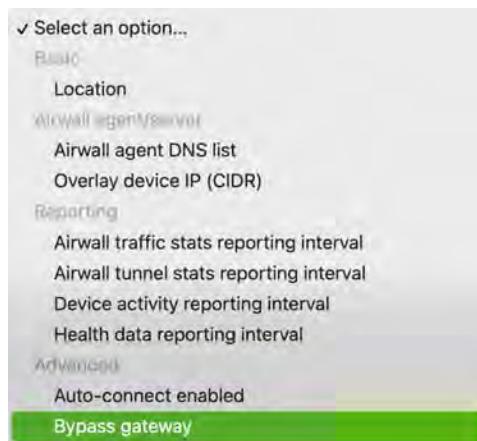
If you set up a bypass Airwall Gateway and set it as the default in the Conductor (see [\(Optional\) Select a default Bypass Airwall Gateway](#) on page 335), all v3.0 Airwall Gateways automatically use the default as needed. If you want an Airwall Gateway to use a specific one instead of the default, or if you haven't selected a default, here's how.

1. Go to **Airwalls** and open an Airwall Gateway that you want to use a bypass Airwall Gateway.
2. Set a bypass gateway to use:
 - a) Go to the **Airwall gateway** tab and select **Edit Settings**.
 - b) Under **Advanced settings**, next to **Use bypass gateway**, select a specific bypass Airwall Gateway to use.



- c) Select **Update**.

 **Note:** You can also set this option in bulk. See [Bulk Configuration of Airwall Edge Services](#) on page 314, and choose the Bypass gateway option:



3. In an Overlay, add trust from this Airwall Gateway's local devices to the bypass destination.

Enable DNS lookup for bypass destinations

If you want or need to use a fully-qualified domain name (FQDN) when specifying a bypass destination, you can enable DNS lookup for bypass. An FQDN may be necessary if the bypass destination IP is not static.

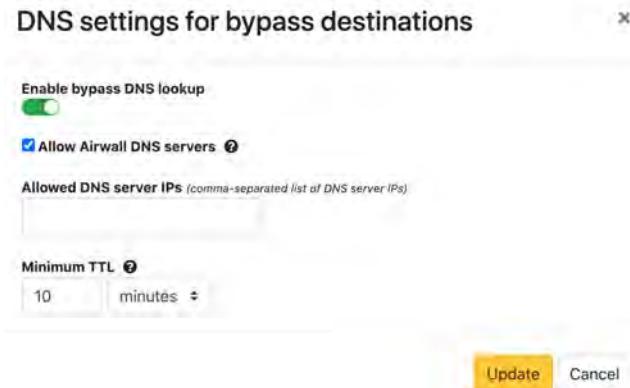
Supported Versions

2.2.10 and later Conductors

Required Role

System administrators

1. Go to **Settings > Bypass DNS**.
2. Select **Edit Settings**.
3. Toggle **Enable bypass DNS lookup** to On.



4. To automatically allow the DNS servers configured on an Airwall Gateway underlay port (instead of listing them under **Allowed DNS server IPs**), check **Allow Airwall DNS servers**. Note this means the DNS servers being used could be different per Airwall Gateway. You also need to set trust to the DNS server on the overlay.
5. Under **Allowed DNS server IPs**, enter trusted DNS server IPs that you want bypass destinations to have access to for DNS lookup. Separate IPs with commas.
6. Under **Minimum TTL**, change the minimum amount of time to accept traffic from resolved IP addresses.
7. Select **Update**.

You can now use an FQDN when specifying a bypass destination. See step 4 under [Seamless Bypass](#) on page 329.

Airwall Edge Service High Availability (HA)

High Availability (HA) Airwall Gateways provide hardware redundancy in a hot-standby mode. Airwall Gateways installed in an HA configuration maintain a heartbeat on a dedicated Ethernet link where only the current primary is participating in overlay network communications. If the primary fails to send heartbeat messages to the secondary, the secondary takes over overlay network communications for the HA pair.

Configure High Availability Airwall Gateways (v2.2.8 and later)

Configuring high-availability (HA) Airwall Gateways in v2.2.8 and later. For v2.2-v2.2.5, see [Configure High Availability for Airwall Gateways \(v2.2-v2.2.5\)](#) on page 341.

The high-availability architecture for Airwall Gateways distinguishes between the following Airwall Gateway roles:

- *Primary vs. secondary:* These roles are assigned when the HA pairing is created. The Primary Airwall Gateway is the one that is added to the overlay in the Conductor. The secondary Airwall Gateway has no configuration on its own with the exception of identity-related information and port configuration. The primary and secondary role assignment can't be changed during the lifetime of the HA pairing.
- *Active vs. standby:* At any given time only one Airwall Gateway is active and participating in overlay network communications. The active Airwall Gateway maintains a heartbeat on a dedicated Ethernet link. If the active Airwall Gateway fails to send heartbeat messages to the standby, the standby takes over the overlay network communications for the HA pair.

Before You Begin

Before you configure a High-availability (HA) pair, you must:

- Have a Conductor set up and running.

- Configure and connect the physical or virtual v2.2.8 or later Airwall Gateways you wish to configure for high availability. You need two physical or two virtual Airwall Gateways. See [Set up physical Airwall Gateways](#) on page 237 for more information.
- Connect both Airwall Gateways to the same underlay and overlay network.



Note: Cloud Airwall Gateways do not support HA.

Create a High-availability Airwall Gateway pairing

High availability Airwall Gateway pairing is supported in v2.2 and later.

To configure High-availability Airwall Gateways, you need to:

- For virtual Airwall Gateways only** – Add an ethernet port
- Connect the Airwall Gateways
- Pair the Airwall Gateways for High Availability
- Make sure the Overlay Port Group settings match

These steps are described in more detail below.

1 For Virtual Airwall Gateways only – Add an ethernet port

For virtual Airwall Gateways, you need to add an ethernet port for the heartbeat the high-availability Airwall Gateways use to communicate status. See your Hypervisor for instructions on adding a network port.

2 Connect the Airwall Gateways

You can configure a pair of physical or virtual Airwall Gateways as a high-availability pair.

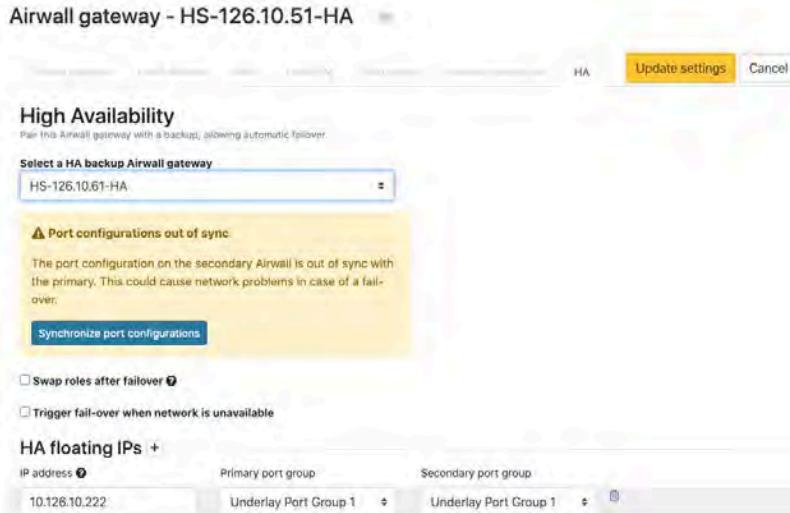
- Select the primary Airwall Gateway and select or add an HA Port Group
 - At the top right of the **Ports** tab, select **Edit Settings**.
 - Select an available HA Port Group, or, to create one, go to **Ports** and select an available port, and create an HA Port Group. The port group sets up a virtual connection between the Airwall Gateways you're configuring as an HA pair. A virtual Airwall Gateway is expandable up to six (6) ports. You must configure one port for HA heartbeats with the HA role.
- Repeat step 1 with the secondary Airwall Gateway.
- If you are using physical Airwall Gateways**, physically connect the primary to the secondary using an ethernet cable between the dedicated HA ethernet ports on both Airwall Gateways with an ethernet cable (so you have both a port and a physical connection between the two Airwall Gateways).
- If you are using virtual Airwall Gateways**, connect the port created above to each other in the virtual network. See your Hypervisor help for instructions.

Next, you'll pair the Airwall Gateways.

3 Pair the Airwall Gateways for High Availability

- Open the page for the Airwall Gateway you want to be Active in the HA pairing.
- Open the **HA** tab and select **Edit Settings**.
- Under **Select a high-availability backup** Airwall Gateway, select the secondary/standby Airwall Gateway.
- If the port configuration on the selected secondary Airwall Gateway is different from the configuration on the primary Airwall Gateway, you'll see an alert with the option to transfer the configuration of the primary Airwall

Gateway to the secondary Airwall Gateway. Select **Synchronize port configurations** to copy the configuration from the primary to the secondary Airwall Gateway.



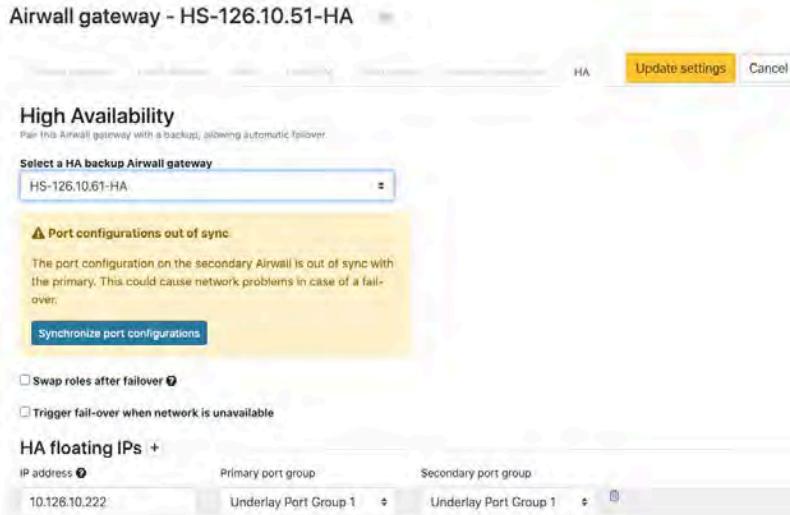
5. Check **Swap roles after failover** if you want the standby Airwall Gateway to remain active in the event of a failover. If this is not checked, the failed Airwall Gateway will automatically become active again once it back online.
6. Check **Trigger fail-over when network is unavailable** if you want to initiate a failover if the Airwall Gateway detects that it has no network connectivity. With this option checked, the standby will become active if the current active Airwall Gateway has no underlay connectivity on any underlay port group but the standby still does.
7. Under **IP address**, enter an available IP address to act as the shared HA IP address for the High Availability pair (see note below).
8. Select an underlay port group for both Airwall Gateways. If you use multiple underlay port groups, you can repeat this step to add HA IP addresses for additional port groups.
9. Select **Update Settings**.

The shared High Availability (HA) IP address is a virtual IP address that moves between the two Airwall Gateways and is only set on the active one, so that remote Airwall Gateways have a consistent destination IP address for their connections to the HA Pair. The shared HA IP address must be a static IP address assigned for this specific purpose.

4 Make sure the Overlay Port Group settings match

1. Check the **Overlay Port Group** of your primary Airwall Gateway for an IP address or any other configured settings (such as DHCP, source NAT, etc).

- The Conductor displays an alert on the **Port configuration** and **HA** tabs if there are discrepancies between the port configurations. Click **Synchronize port configurations** to replicate the configuration of the primary Airwall Gateway to the secondary. Note that the secondary Airwall Gateway must be online to replicate the settings.



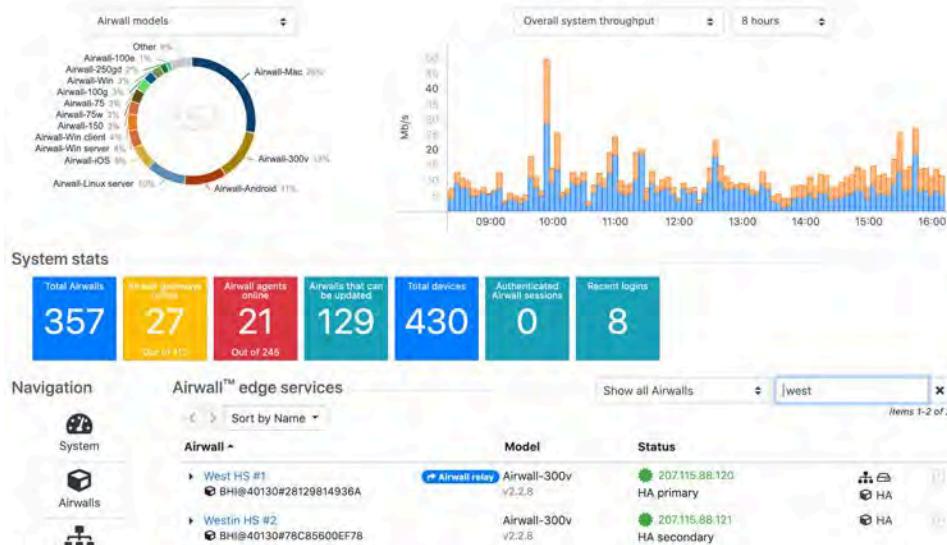
Test the High-Availability Pair

The **HA** tab on either HA-paired Airwall Gateway displays the setup of the HA pair, identifying the primary and secondary, along with their current roles and status. Immediately after setting up the HA pair, the status displays **Setting up**. After a few seconds, the status of both Airwall Gateways will change: to **OK (tunneling)** on the active and to **OK (monitoring)** on the standby.

HA Configuration	
300Hv-5.20.71-SrcNAT-DUT	300Hv-5.20.72-SrcNAT-DUT
HA Setup	HA primary
Role	Active
Status	OK (tunneling)
HA Link	UP
	Swap Roles

You can manually reverse the active and standby roles by selecting **Swap Roles**. This option initiates a failover from the current active Airwall Gateway to the standby, and permanently reverse the roles irrespective of the **Swap roles after failover** setting.

You can also see that the Airwall Gateways are paired on the Dashboard.



Remove a High-Availability Pairing

You remove an HA pairing from the primary Airwall Gateway.

1. Open the page for the primary Airwall Gateway, and on the **HA** tab, select **Edit Settings**.
2. Select **Remove HA pairing**.
3. Select **Update Settings**.

When an HA Pair is removed, the primary Airwall Gateway stays in the Overlay Network and the secondary Airwall Gateway is removed from the Overlay network.

Configure High Availability for Airwall Gateways (v2.2-v2.2.5)

Configuring high-availability (HA) Airwall Gateways in v2.2-v2.2.5. For v2.2.8 and later, see [Configure High Availability Airwall Gateways \(v2.2.8 and later\)](#) on page 337.

Before You Begin

Before you configure a High-availability (HA) pair, you must:

- Have a Conductor installed
- Configure and connect the physical or virtual v2.2 to v2.2.5 Airwall Gateways you wish to configure for high availability. You need two physical or two virtual Airwall Gateways. See [Set up physical Airwall Gateways](#) on page 237 for more information.



Note: Cloud Airwall Gateways do not support HA at this time.

To create a high-availability Airwall Gateway pairing

To configure High-availability Airwall Gateways, you need to:

1. **For virtual Airwall Gateways only** – Add an ethernet port
2. Connect the Airwall Gateways
3. Pair the Airwall Gateways for High Availability
4. Make sure the **Overlay Port Group** settings match

These steps are described in more detail below.

- 1 For Virtual Airwall Gateways only – Add an ethernet port

For virtual Airwall Gateways, you need to add an ethernet port for the heartbeat the high-availability Airwall Gateways use to communicate status. See your Hypervisor help for instructions on adding a network port.

- 2 Connect the Airwall Gateways

You can configure a pair of physical or virtual Airwall Gateways as a high-availability pair.

1. Select the primary Airwall Gateway and select or add an HA Port Group
 - a) At the top right of the **Ports** tab, select **Edit Settings**.
 - b) Select an available HA Port Group, or, to create one, go to **Ports** and select an available port, and create an HA Port Group. The port group sets up a virtual connection between the Airwall Gateways you're configuring as an HA pair. A virtual Airwall Gateway is expandable up to six (6) ports. You must configure one port for HA heartbeats with the HA role.
2. Repeat step 1 with the secondary Airwall Gateway.
3. **If you are using physical Airwall Gateways**, physically connect the primary to the secondary using an ethernet cable between the dedicated HA ethernet ports on both Airwall Gateways with an ethernet cable (so you have both a port and a physical connection between the two Airwall Gateways).
4. **If you are using virtual Airwall Gateways**, connect the port created above to each other in the virtual network. See your Hypervisor instruction.

Next, you'll pair the Airwall Gateways.

3 Pair the Airwall Gateways for High Availability

1. Select the **HA** tab and click **Edit Settings**.
2. Under **Select a high-availability backup** Airwall Gateway, select the secondary Airwall Gateway.
3. Under **IP address**, enter an available IP address to act as the shared HA IP address for the High Availability pair (see note below). You may need to select a Primary port group as well.
4. Click **Update Settings**.
5. If you want to swap the primary Airwall Gateway with the secondary one, go to the **HA** tab, and by **Role**, select **Swap Roles**.

The shared High Availability (HA) IP address is a virtual IP address that moves between the primary and secondary Airwall Gateways, so that remote Airwall Gateways have a consistent destination IP address for their connections to the HA Pair. The shared HA IP address must be a static IP address assigned for this specific purpose.

4 Make sure the Overlay Port Group settings match

1. Check the **Overlay Port Group** of your primary Airwall Gateway for an IP address or any other configured settings (such as DHCP, source NAT, etc).

2. If there are settings there, copy them to the standby Airwall Gateway's **Overlay Port group**.

Airwall - HS-126.10.41

Airwall Local devices Ports Reporting Diagnostics Intrusion prevention HA Edit se

Port configuration Failover settings Serial over IP

Ports

Port 1	Port 2	Interfaces	Assigned	IP address	MAC	MTU	VLAN
		Port 1	<input checked="" type="checkbox"/>	10.126.10.41/24	00:50:56:b0:7e:3a	1500	

Port groups

- Underlay group** Underlay Port Group 1
- Overlay group** Overlay Port Group 1

Name	Interfaces
Overlay Port Group 1	Port 2

IP addresses	Type	IP address	Gateway
Static	IPv4	10.126.1.4/24	

Enable source NAT	Enable MAC masquerading	DHCP settings	Configure...
<input checked="" type="checkbox"/>	No	None	

Static routes

None

Test the High-Availability Pair

In either HA paired Airwall Gateway, on the **HA** tab under **Status**, notice the screens are trying to talk to each other. The primary status is **OK (tunneling)** and the secondary status is **OK (monitoring)**.

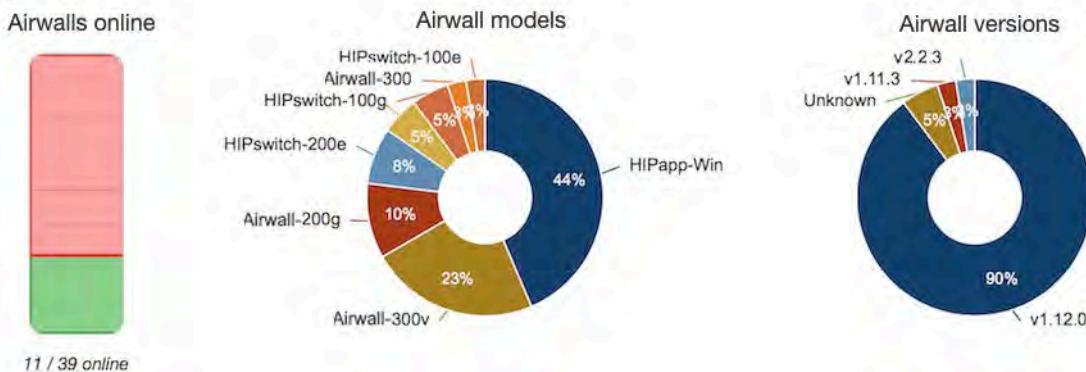
300Hv-5.20.71-SrcNAT-DUT is an HA primary currently paired with 300Hv-5.20.72-SrcNAT-DUT

HA floating IPs 10.5.20.7
Last failover None

HA Configuration	
300Hv-5.20.71-SrcNAT-DUT	300Hv-5.20.72-SrcNAT-DUT
HA Setup	HA primary
Role	Active
Status	OK (tunneling)
HA Link	UP

You can also see that the Airwall Gateways are paired on the Dashboard.

Dashboard



11 / 39 online

Airwall™ edge services

Airwall	Model	Status	Actions
300Hv-5.20.71-SrcNAT-DUT ■ BH@40130#D78FF6B4A3C5	Airwall-300v v2.2.3	10.5.20.7 HA primary	⋮ ⌂ 🔒 %
300Hv-5.20.72-SrcNAT-DUT ■ BH@40130#CC3D6582DB85	Airwall-300v v2.2.3	10.5.20.72 HA secondary	⋮ ⌂ 🔒 %
300Hv-5.30.71 ■ BH@40130#715AB913BB5	Airwall-300v v2.2.3	10.5.30.71	⋮ ⌂ 🔒 %
300Hv-5.30.72 ■ BH@40130#C0732CB6318D	Airwall-300v v2.2.3	10.5.30.72	⋮ ⌂ 🔒 %

Display revoked Airwalls

Remove a High-Availability Pairing

You can remove an HA pairing from the primary Airwall Gateway.

- In the primary Airwall Gateway, on the **HA** tab, click **Edit Settings**.
- Click **Remove HA pairing**.

When an HA Pair is removed, the primary Airwall Gateway stays in the Overlay Network and the secondary Airwall Gateway is removed from the Overlay network.

One-arm mode

You can configure an Airwall Gateway to use a single network connection in cases where you want to prevent common routing errors caused by multiple interfaces.

One-arm mode is simple to configure, but consider the following before configuring an Airwall Gateway in one-arm mode.

- You cannot place an Airwall Gateway in transparent mode while in one-arm mode
 - You must use a wired port. One-arm mode will not function using a wireless or cellular interface.
 - The overlay IP and netmask in **Local Devices -> Device Network Configuration** is ignored; however, the information is retained if you revert your settings from one-arm mode later.
 - Overlay routes on the **Local Devices** tab are also ignored but retained if you revert.

Configure one-arm mode

To configure an Airwall Gateway for one-arm mode:

1. Select the desired Airwall Gateway from the **Airwalls** tab in the Conductor.
2. Select the **Airwalls** tab and click **Edit Settings**
3. In the **Advanced Configuration** section, uncheck **Enable spanning tree protocol**
4. Click **Update Settings**
5. Select the **Local Devices** tab and click **Edit Settings**
6. In the **Configuration** section, uncheck **Enable device discovery**
7. In the **Device Network Configuration** section, uncheck **Enable NAT** and **Enable source NAT**
8. In the **Local Device DHCP** section, uncheck **Enable DHCP server**
9. Click **Update Settings**
10. Select the **Ports** tab and then **Shared Network**
11. Click **Edit Settings**
12. In the **Port 1** section, select **Static** from the **Protocol** drop-down and enter the IP address, netmask, and any other required fields for your shared network
13. Click **Update Settings**



Note: You will get a message that the Airwall Gateway is reconnecting.

Once the configuration process is complete, you'll get a Network configuration successful message.

14. Select the **Port** assignment tab and click **Edit Settings**
15. For **Port 1**, select **Dual-Use (Shared + Device)** from the **Assigned to** drop-down
16. For **Port 2**, select **Disabled** from the **Assigned to** drop-down
17. Click **Update Settings**
18. In the **Confirm Dual-Use Port Configuration** dialog, click **OK**
19. The Airwall Gateway will re-configure and you will receive the same messages you received when configuring the port assignments

Your Airwall Gateway is now correctly configured for dual-use mode.

Network address translation (NAT)

Network Address Translation (NAT) translates an IP address in one network to a different IP address in another network. The two IP addresses are referred to as the External IP address and the Internal IP address. The External IP address is the IP address of the device in the overlay network and the Internal IP address is the actual IP address of the device.

NAT is used in conjunction with Airwall Gateway subnet routing. To use NAT, the private IP address of a local device must be in a different subnet than the public IP address of a remote device. For example, if a local device's private IP address is 192.168.56.99, the device cannot be reached by a remote device that is configured with a public IP address of 192.168.56.xxx, assuming a subnet mask of 255.255.255.0.

To enable NAT on a device or multiple devices:

1. Go to **Airwalls** and select the Airwall Gateway to which the device or devices belong.
2. Select **Local Devices** and click **Edit Settings**.
3. Check **Enable NAT** and enter the gateway external IP address.
4. Click **Update Settings** to save the configuration.

The screenshot shows the Airwall configuration interface. At the top, there are tabs for Airwall, Local devices, Ports, Reporting, Diagnostics, Intrusion prevention, and HA. Below these are two sub-tabs: Configuration (selected) and Port filtering. The main area is titled "Local Devices" and contains a table with columns: Device name, External IP, Internal IP, and a delete icon. A row shows "EB1-IN1" with "192.168.56.103" in both the External and Internal IP fields. To the right of the table are sections for "Device Discovery" (with "Enable device discovery" checked), "Device Network Configuration" (with "Overlay IP" set to 192.168.56.2, "Overlay Netmask" set to 255.255.255.0, and "Enable NAT" checked), "Local Device DHCP" (with "Enable DHCP server" checked), and "Overlay Routes" (which is empty). A note at the bottom states "No device network routes defined for this HIPswitch".

Encryption and tunnel compression on an Airwall Gateway

You can change the encryption or compression of Airwall Gateways.

1. Go to **Airwalls** and select an Airwall Gateway.
2. Click **Edit Settings**.
3. In the **Advanced settings** section, select one of the following from the **Default encryption** drop-down:
 - AES-256-GCM and compression
 - AES-256-GCM
 - AES-256-CBC and compression
 - AES-256-CBC



Note: Enabling compression may result in improved throughput

4. Click **Update Settings**.



Important: If the encryption or compression settings of two communicating Airwall Gateways differ, the settings of the peer Airwall Gateway are used by default.

Protected devices with static routing

You can configure static routing for protected devices with IP addresses not directly connected to an Airwall Gateway.

To use static routing :

1. Go to **Airwalls** and select an Airwall Gateway.
2. Select **Ports** and click **Edit Settings**.
3. Click **+ Add route** and enter the target network in CIDR format and gateway.
4. Add additional routes as necessary by repeating the previous step.

5. Click Update Settings.

Protected devices with DHCP

If you have protected devices that use DHCP to obtain an IP address, you need to configure DHCP on the Airwall Gateway that protects that device.



Note: You must have an overlay gateway IP address on the Overlay port group on which you are enabling DHCP.

To use DHCP to configure protected devices with IP addresses:

1. On the **Airwalls** page, select the Airwall Gateway to which the device or devices belong.
2. On the **Ports** tab, open the Overlay you are enabling DHCP on.
3. Under **DHCP Settings**, click **Configure**.
4. Under **DHCP Configuration**, select **DHCP server**.
5. Enter the range of IP addresses in the Start and End boxes.
6. Enter the netmask.
7. Under **Gateway**, enter the IP address of the Airwall Gateway.
8. Optional. Enter DNS server information, if required.
9. Click **Apply**.

Protected devices are now dynamically assigned IP address when connected to the Airwall Gateway.

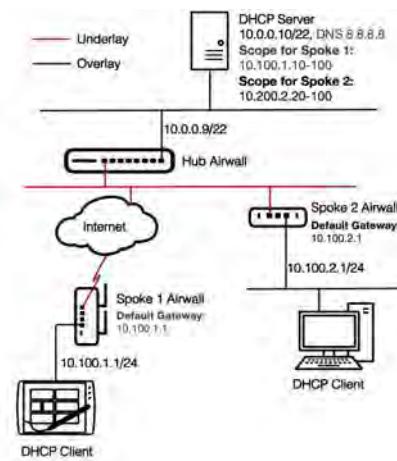
DHCP relay on an Airwall Gateway

If you have protected devices that use DHCP to obtain an IP address, you can configure the Airwall Gateway to relay the DHCP address to your DHCP server.



Note: You must have an overlay IP address on the Overlay port group of the Airwall Gateway that has your DHCP clients behind it (10.100.2.1/24 in the diagram below). This overlay IP address should be the default gateway that is handed out by the DHCP Server for the DHCP clients..

Deploy the DHCP server so it routes traffic to DHCP-relay-enabled spokes via the hub Airwall. The DHCP server needs to connect to an Overlay port and the DHCP relay traffic needs to traverse the tunnel to the Spoke Airwall, as shown in the following diagram.



1. Make sure that the DHCP server is a protected device of the hub Airwall Gateway.

2. For each Airwall Gateway (Spoke 1 and Spoke 2 in the diagram) that has a DHCP device behind it:
 - a) From the **Airwalls** page, open the Airwall Gateway to which the DHCP client device or devices belong.
 - b) On the **Ports** tab, open the Overlay you are enabling DHCP on.
 - c) Under **DHCP Settings**, click **Configure**.
 - d) Under **DHCP Configuration**, select **DHCP relay**.
 - e) Set the **Upstream DHCP server** (for example, 10.0.0.10).
 - f) Click **Apply**.
3. Add a network object that includes the DHCP scope as a protected device to each Spoke Airwall Gateway. For example, for Spoke 2, add a device with IP Address = 10.100.2.0/24 (this is referred to as a Network Object).
4. Create an Overlay for the DHCP traffic:
 - a) On the **Overlays** page, select **New overlay network**. Select **Manual**, name the Overlay, and select **Finish**.
 - b) On the **Devices** tab, click the + and add the network object created in step 3 (that is, 10.100.2.0/24) to the Overlay.

Local devices				
Devices	Overlay device IP (NAT)	Overlay device IP	MAC	Activity
Network Object	10.100.2.0/24	10.100.2.0/24		None

- c) Add the DHCP server (10.0.0.10 in the diagram) to the Overlay.
- d) Establish trust between the network object and the DHCP server.

Trust	Device name	Overlay IP	MAC address	OUI	Airwall
○ ○	DHCP Server	10.0.0.10		Hub	
○	Network Object	10.100.2.0/24			Spoke 1



Note: The DHCP Scope Default gateway (i.e 10.100.2.1) needs to match the Overlay IP for the port group connected to DHCP clients. And, the subnet mask of the DHCP scope must match the subnet mask of the Overlay IP port group.

Firewall on an Airwall Gateway

Each Airwall Gateway has a Stateful Packet Inspection (SPI) Firewall that can be configured in the Conductor. Communications from remote devices behind remote Airwall Gateways are incoming connections. When the Airwall Gateway firewall is enabled, all incoming communications coming from remote Airwall Gateways are blocked by default, unless they are related to an already established session from a local device behind the local Airwall Gateway.

To enable the firewall on an Airwall Gateway:

1. Click **Airwalls**, select an Airwall Gateway.
2. Go to **Local Devices > Firewall**.
3. Click **Edit Settings**, and then click **Enabled** to view and configure the Firewall settings.

You can enable or disable the firewall, enable or disable Incoming ICMP Protection, and enable or disable SYN Flood Protection. Once configured, click **Update Settings** to save the settings.

Limit Device Traffic on an Airwall Gateway with Port Filtering

You can use Airwall Gateway port filtering to limit what traffic can pass over an Overlay based on TCP/UDP Ports. With port filtering enabled, all communication from remote to local devices is disabled, and you create custom rules to tell the local Airwall Gateway what to allow as incoming connections to local devices.



Note: When removing a port filtering rule that allows connections, any ongoing connections at the time the rule is deleted are not blocked. Rules are checked when a new connection is attempted.



Note: To establish communication between local and remote devices, you must also [Add and remove device trust](#) on page 360 on the overlay, in addition to specifying custom port filtering rules

Remote Device communication

Remote devices are devices that are behind different Airwall Gateways and are reachable in the overlay network. Remote devices send connection requests to local devices, and typically use random port numbers for their connection attempts, so typically you leave the remote device port range blank.

Local Device communication

Local devices are devices that are connected locally to the Airwall Gateway you are configuring. Local devices receive incoming connections from remote devices. Most local device services are listening on a specific port or ports that you typically specify as part of the custom rule.

TCP or UDP protocol

You can specify TCP or UDP as the underlying communication protocol used by devices. If you are using a different IP protocol, select **IP (any)** from the Protocol list, which allows devices to use any IP protocol.

What happens to Port Filtering Rules when you delete devices?

When you delete local devices from an Airwall Gateway or delete remote devices from remote Airwall Gateways, the port filtering rules associated with the devices are deleted. If you remove an Airwall Gateway from the overlay network, the rules associated with the Airwall Gateway are labeled `not_reachable`.

How to set up Port Filtering

1. In Conductor, open the page for the Airwall Gateway you want to set up Port Filtering in.
2. Open the **Local devices** tab, and **Port filtering** subtab, and click **Edit Settings**.

- Under **Enable port filtering**, select **Enabled**.

Configuration **Port filtering**

With port filtering enabled, all communication from remote to local devices is disabled. Use the custom rules to enable incoming communication.

Enable port filtering

Enabled **Disabled**

Allow incoming pings (ICMP)

Enabled **Disabled**

SYN flood protection

Enabled **Disabled**

Custom rules

Add custom traffic whitelisting rules to enable communication among specific devices.

Enabled	Remote device and port range	Local device and port range	Protocol
<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/> Any	<input checked="" type="checkbox"/> IP (any)

Note: With port filtering enabled, all communication from remote to local devices is disabled, and you create custom rules to tell the local Airwall Gateway what to allow as incoming connections to local devices.

- To allow remote devices to ping local devices, enable **Allow incoming pings (ICMP)** to allow remote devices to ping local devices.
- If you need to protect against Denial-of-service attacks, enable **SYN flood protection**.
- Under **Custom rules**, select **Add Rule** and set up the rules to allow traffic between the local devices behind this Airwall Gateway and remote devices behind other Airwall Gateways:
 - Under **Remote device and port range**, select one or more remote devices you want to be able to communicate with local devices. Since remote devices usually use random port numbers when they attempt to connect, most of the time, leave the port range blank.
 - Under **Local device and port range**, select one or more local devices you want to communicate with the selected remote devices. Since local device ports usually remain the same, specify the port range for the local devices.
 - Under **Protocol**, if you are using TCP or UDP, specify the underlying communication protocol used by devices. If you are using a different IP protocol, select **IP (any)** from the **Protocol** list, which allows any IP protocol to be used.

Custom rules

Add custom traffic whitelisting rules to enable communication among specific devices.

Enabled	Remote device and port range	Local device and port range	Protocol
<input checked="" type="checkbox"/>	Any	Any	<input checked="" type="checkbox"/> IP (any) <input type="checkbox"/> TCP <input type="checkbox"/> UDP

- Select **Add Rule** to add additional rules, as needed.
 - When you are finished creating rules, select **Update Settings** to save your port filtering settings.
- You must also add devices to an Overlay and establish trust before communication is fully enabled. See [Add and remove device trust](#) on page 360.

For more information on Port Filtering, see [Limit Device Traffic on an Airwall Gateway with Port Filtering](#) on page 348.

Spanning Tree Protocol on the Overlay Network

Overview

Airwall Gateways can emit and participate in Spanning Tree Protocol (STP), helping reduce network loops and allowing for link redundancy.

How an Airwall Gateway interacts with existing STP infrastructure varies depending on the installed firmware version.

1.12.4 - 1.12.6

Airwall Gateways/HIPswitches running versions 1.12.4 through 1.12.6 have STP enabled on the overlay network interface by default. It is not configurable or able to be disabled.

STP bridge priority is 32768

2.0.x

Airwall Gateways/HIPswitches running versions 2.0.x provide an option to disable STP if not needed. The feature is enabled by default.

STP bridge priority is 32767.

2.1.x

Airwall Gateways/HIPswitches running versions 2.1.x or greater will not enable STP if there is only one network interface configured for the overlay network. By default, -100 and -200 series Airwall Gateway/HIPswitches enable the feature.

Note: Conductor provides a setting to enable or disable STP for these platforms; however, this has no affect to the running unit, as it will not enable.

STP bridge priority is 61440.

Recommendations

If multiple network interfaces are configured with the Underlay role, they are put into a bridge, and STP is enabled. STP on this bridge does is not configurable, nor can it be disabled.

Connect and Configure Devices

As you prepare to connect devices to Airwall Gateways, you may want your Airwall Gateway product guide available to identify the ports reserved for connecting devices you want to protect.

Different Airwall Gateway models support different numbers of devices, and some older models may use different port names such as:

- Device Network
- Private Network
- Equipment Network



CAUTION: Avoid duplicate device IP addresses, even if the devices are members of different Overlay networks. If more than one Airwall Gateway is a member of both Overlay networks, it creates an unresolved network routing conflict.

Add devices to the Conductor

After you connect devices to Airwall Gateway hardware, there are four ways to add a device to the Conductor.

- [Enable passive device discovery](#) on page 352
- [Detect devices manually](#) on page 352
- [Import and export devices using a CSV file](#) on page 352
- [Add devices manually](#) on page 354

If you are working with a large number of devices, you may want to create device groups for ease of administration, once the devices have been added to Conductor. See [Use device groups and smart device groups](#) on page 354 for more information on creating groups.

Use device discovery

Airwall Gateways are able to auto discover devices as soon as they are plugged in. Please note however, a discovered device cannot communicate with other devices in an overlay network until an administrator explicitly accepts the device.

There are two different ways to enable device discovery:

1. [Enable passive device discovery](#) on page 352
2. [Detect devices manually](#) on page 352

Enable passive device discovery

Enabling device discovery option allows an Airwall Gateway to passively discover devices within the overlay device network it is connected to.

To enable device discovery:

1. Go to **Airwalls** and select an Airwall Gateway.
2. Go to **Local Devices > Configuration** and click **Edit Settings**.
3. Select your version:
 - **In v3.0 and later** – Under **Settings**, check **Enable passive device discovery**.
 - Before v3.0 – In the **Device Discovery** section on the right, check **Enable device discovery**.
4. Select **Update Settings**.

Detect devices manually

To use passive device detection, enable **Passive device discovery** and set up **Device Network Configuration** for the Airwall Gateway.

1. Go to **Airwalls** and open an Airwall Gateway from the list.
2. Go to **Local devices > Configuration**, and right of **Local devices**, open the **Other actions** menu and select **Detect devices**.

Once detected, the protected device appears in the Conductor and the device can then be added to your Overlay networks.

You can also delete detected devices by opening the **Other actions** menu and selecting **Delete discovered devices**

Import and export devices using a CSV file

Device import and export is useful if you have a large number of devices to manage in your Airwall deployment.

A .csv file contains plain text data sets separated by commas with each row consisting of one or more fields.



Note: Importing devices is not destructive, it is additive - so devices in the import are added, but none are deleted.

To make the management of your devices easier, you can download a device import .csv template from [here](#), export and modify the existing device file, or create the file yourself. A typical .csv file looks like the following example:

```
airwall_id,device_name,overlay_device_ip,overlay_device_ip_nat,mac_address,mac_lockdown
BHI@40130#35C1B68998D9,,Local
  Workstation,192.168.59.101,,08:00:27:05:03:2e,,FALSE
BHI@40130#4F6B8FD47B90,,Local Workstation
  2,192.168.59.102,,08:00:27:67:e6:6e,,FALSE
```

The first line contains field names with each successive line containing data corresponding to the fields.

airwall_id	This is the UID of the Airwall Edge Service you want your devices to use. You can find this information in the UID field for the Airwall Edge Service in the Conductor. The UID looks like this: BHI@40130#101E20100067
device_name	A friendly name for the device.
overlay_device_ip	The IP address of the device.
overlay_device_ip_nat	(Optional) If your network topology requires you also use NAT you can enter the internal IP address here.
mac_address	(Optional) Enter the MAC address of your device. This field is required if you want to enable MAC lockdown (<i>mac_lockdown=TRUE</i>).
mac_lockdown	Enter TRUE if you require static addressing for the device, otherwise enter FALSE.

Import devices using a .csv file

You can import devices into your Conductor using a .csv file.



Note: You cannot import emojis using the .csv file.

1. If you want to use the template .csv file, go to **Devices** and from the **Other Actions** menu, select **Export devices template**. Add devices by adding rows to the template, following the column headers detailed above.
2. Go to **Devices** and from the **Other Actions** menu, select **Import devices list**.
3. Select **Choose File** and then open the .csv file containing your device list.



4. Click **Upload** and the devices will be listed, grouped by their associated Airwall Edge Services.



Note: If you receive any errors, correct the .csv file and try to import it again.

5. Select **Next**, review the results, and then select **Commit**. When it's done, select **Finish**.

Export devices to a .csv file

Export the devices in the Conductor to a .csv file.

1. Go to **Devices** and from the **Other Actions** menu, select **Export devices list**.
2. Select **Export** to confirm.

Add devices manually

You can manually add devices in the Airwall Gateways tab.

1. Go to **Airwalls** and select an Airwall Gateway from the list.
2. Go to **Local Devices** and click **Add Device**.
3. In the dialog, enter a device name, IP address, and optionally a MAC address.
4. Click **Create**.



Note: Adding devices from the **Airwalls** list is also possible. Select the drop-down to the right of an Airwall Gateway, and click **Add Device**.

Use device groups and smart device groups

Device groups streamline the management of a large number of devices, allowing you to manage them as a group. Note that a device group does not create device trust policy between them. See [Configure Device Trust](#) on page 360.

There are two types of device groups:

- **Standard** – Create standard device groups to manage the devices in them manually. See [Create standard device groups](#) on page 87.
- **Smart** – Use Smart Device Groups to greatly simplify the creation and management of large groups of devices. Dynamically add devices to a group by defining rules to create a Smart Device Group. Rules can match criteria such as organizational hierarchy, geographic location, or network domain. When you create a Smart Device Group, any new devices that match the rules you defined are added to the group automatically. See [Manage devices dynamically with Smart Device Groups](#) on page 87.

Wildcard Devices

Some overlay network configurations require allowing all traffic inbound or outbound to a specific IP. This can be accomplished with a wildcard 0.0.0.0 network device.

Applies to:

2.1.3 and above

A 0.0.0.0 device functions as a wildcard, and when configuring trust, selecting the 0.0.0.0 device applies the trust policy to all devices behind the parent Airwall Gateway. However, there are several things to consider when planning a configuration that uses the 0.0.0.0 wildcard device.

- Each overlay network can only have one 0.0.0.0 address to avoid the possibility of IP address conflicts.
- If your Airwall Gateway is running a version prior to 2.1.3, overlay networks containing a 0.0.0.0 device cannot use subnet routing or NAT.
- Airwall Gateways running version 2.1.3 or above support subnet routing, NAT, and SNAT. It is recommended all Airwall Edge Services in an overlay network with the 0.0.0.0 wildcard device run version 2.1.3 or later.
- Airwall Agents and Airwall Servers do not support the 0.0.0.0 wildcard device.

How to configure wildcard device

1. Go to **Airwalls** and select an Airwall Edge Service.
2. Add a new device with the IP address set to 0.0.0.0. See [Add devices to the Conductor](#) on page 351 for more information about adding devices.
3. Go to **Overlays** and select the overlay network for which you are configuring trust.
4. On the **Devices** tab, click the button for the 0.0.0.0 device, and then select the other devices and groups in the overlay network that require communications with the devices represented by the 0.0.0.0 wildcard device.

Overlay network default route

Starting in version 2.1.3, Airwall Gateways now support the option of setting a default route on the overlay network. This can be set on a per Airwall Gateway basis under the **Local Devices > Overlay Routes** section.

Advantages of setting a default route on the overlay helps simplify network deployments and architectures where the Airwall Gateway's local devices are in multiple subnets more than one hop away.



CAUTION: If you set an overlay network default route on Airwall Gateways running versions prior to 2.1.3, it might cause internal routing issues, leading to the Airwall Gateway not reporting as online in Conductor.

See also

- https://www.temperednetworks.com/sites/default/files/webhelp/content/topics/support_kb_110.html
- [Wildcard Devices](#) on page 354

Create an overlay network default route

To create an overlay network default route:

1. Navigate to the [Airwalls](#) page and select an Airwall Edge Service.
2. Add a new overlay route with a Target Network Address set to 0.0.0.0/0 and set the Gateway to the next hop gateway.



Note: This next hop gateway needs to be within the same subnet as the subnet used for the Airwall Gateway's **Overlay Gateway IP**.

Create and Manage an Overlay (Protected) Network

Create an overlay (protected) network for your deployment.



Note: To create overlay networks, you must have system administrator privileges in the Conductor.

Before you begin, check that:

- Airwall Gateways are connected to the Conductor, and Airwall Gateway groups are created, if desired. See [Set up physical Airwall Gateways](#) on page 237 for more information.
- Devices are connected to Airwall Gateways and device groups created, if desired. See [Connect and Configure Devices](#) on page 351 for more information.
- Determine whether you want to enable VLAN tagged traffic on the overlay network. See [Allow VLAN tagged traffic in your overlay network](#) on page 356 for more information.
- Determine the users and administrative roles needed to manage the overlay network. See [Edit members of an overlay network](#) on page 356 for more information.

Create an overlay network

The last step in deploying the Airwall secure network is to create an overlay. An overlay is a fabric of secured communications channels that allow trusted devices to communicate securely with each other. Overlays are controlled by Airwall Edge Services and administered by the Conductor.

To create an overlay network:

1. Go to **Overlays** and click **New overlay network**.
2. Enter a name and description (optional) for the overlay network.
3. **In 2.2.10 and later**, if you want the overlay to manage relay rules automatically, enable the **Manage a relay rule based on this overlay network's configuration** option, and choose the Airwall Relays or Airwall Relay groups that you want this overlay to use..
4. Select **Save**.
5. Select the overlay you added and on the **Devices** tab, click the button to the right of **Add devices**.
6. In the **Add Devices** dialog, select each device or device group that you want to add to the overlay network and click **Add Devices**.
7. In the **People** section on the right side of the **Devices** tab, click **Update** to assign managers or members of the overlay network.
8. Optional: Select the **VLAN tagged traffic** tab and select the appropriate options if you want to allow VLAN tagged or untagged traffic.

Basic overlay network creation is now complete. For more information, see the following sections:

Add devices or device groups to an overlay network

Once an overlay network is created, you can add devices or groups of devices.

To add devices to an overlay network:

1. Go to **Overlays** and select an overlay network
2. Click the button to the right of the **Add devices** field and a list of available devices is displayed.



Note: If the name of the device is known, you can enter the device name directly into the text box and a list of matching devices and device groups will be displayed.

3. Select the devices you want to add to the overlay network and click **Add Devices**.

If you have a large number of devices, you may want to consider creating device groups. See [Use device groups and smart device groups](#) on page 354 for more information.



Important: Adding devices to an overlay network does not enable communications to or from that device. To enable communications, you must enable trust between devices. See [Configure Device Trust](#) on page 360 for information on device trust.

Edit members of an overlay network

Overlay networks can only be modified by users who are managers of that network. After creating an overlay network, you may want to add additional managers to your overlay network or edit their roles.

To edit members of an overlay network:

1. Go to **Overlays** and select the overlay network.
2. In **People** click **Update**.
3. The **Add People** dialog displays the list of users. You can add a user as a member or manager by selecting the appropriate column in the list.
4. When finished, click **Close**.

Allow VLAN tagged traffic in your overlay network

If your overlay network needs to support VLAN tagged traffic, you must explicitly allow VLAN tagging:

1. Go to **Overlays** and select an overlay network.
2. In the **Info** section, click **Edit Settings**.
3. In the overlay dialog, click the **VLAN tagged traffic** tab and set the following:
 - a) Specify if tagged or untagged traffic is allowed on your network.
 - b) In **Allowed tags**, enter VLAN tags separated by commas. You may specify tags from 0 to 4095. Leave the field blank if you want to accept any VLAN tag.
4. Click **Save**.

Set up Overlay Port Groups

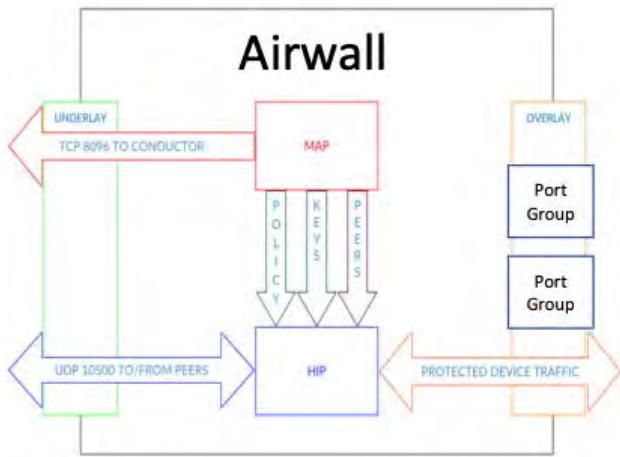
The default port groups work for some deployments. You may need to set up overlay port groups if your deployment requires it.

Overlay Port Groups are used to connect your Airwall Gateway to your protected networks. Airwall Gateways default to having a single overlay Port Group, but you may need to configure your overlay port groups when you want to:

- Micro-segment your network for fine grain security control
- Configure IP addresses or Source NAT (SNAT) for routed deployments
- Set up two Airwall Gateways for High Availability

If your Airwall Gateway is only providing relay functionality, it only needs an Underlay Port Group, and doesn't use any configured Overlay port group.

You can set up multiple port groups for an overlay, assigned to different physical or VLAN tagged sub-interface ports. When multiple ports are included in a Port Group, they are bridged. Port groups are also connected to the overlay through routing and/or bridging.



Get to Know Your Airwall Gateway Ports

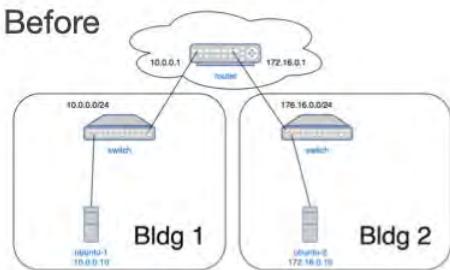
Here's how the physical ports are assigned on most Airwall Gateways:

- Port 1 – Connects to the initial underlay network, and is assigned to the underlay Port Group.
- Port 2 & Up – Connect to overlay networks, and are assigned to an overlay Port Group.

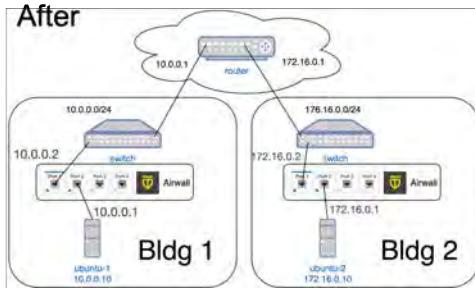


Basic Airwall Gateway Deployment

The most basic Airwall Gateway deployment design is to put Airwall Gateways inline in front of protected devices. If you don't want to, or can't, change IP addresses, you replicate the default gateway of the router on the overlay Port Group. (If these devices are using DHCP, see [Protected devices with static routing](#) on page 346 to configure DHCP on the overlay port group.)



The underlay IP address can be any address on the network. DHCP is common, or you can configure a static IP if needed. The overlay IP address is the same as the default gateway on the router.



Set up an Overlay Port Group

By default, an Airwall Gateway has two port groups. One underlay port group assigned to Port 1 and one overlay port group assigned to the remaining ports. On virtual and cloud Airwall Gateways, you may be able to configure more ports if supported by the virtual or cloud platform.

1. In the Conductor, go to the Airwall Gateway on which you want to set Port Groups, open the **Ports** tab, and select **Edit Settings**.
2. Select an Overlay port group you want to use, or add a new port group by clicking the + to the right of **Port groups**, and select **Overlay group**.

3. Click the arrow on the left of your **Overlay group** header to expand the settings for that Port Group.

4. Enter a name for the group, and under **Interfaces**, select the ports or other interfaces for the group.
5. Under **IP addresses**, click the + to add IP addresses. For example, 10.0.1.1/24 (be sure to include the prefix length). Your protected devices will use this address as their gateway to reach the rest of your overlay network.
6. Select the network options that apply for your implementation:
 - a) **Enable Source NAT** – Check this box to rewrite the source IP address of traffic arriving from other port groups or tunnels with the overlay IP address of this port group. You must also configure an overlay IP address. Use this option when your local protected devices do not use this Airwall Gateway as their default gateway. This setting enables connections, permitted by policy, from remote overlay devices to local protected

devices. When you enable Source NAT, local protected devices cannot initiate connections to remote overlay devices.

- b) **Enable MAC masquerading** – Check this box to rewrite the source MAC address of all traffic arriving from other port groups or tunnels with the Airwall's MAC address. Use this option if the network you are connected to doesn't permit foreign MAC addresses. Note: Checking the Routed traffic only box enables MAC masquerading by default.
- c) **Enable spanning tree protocol** – Leave this box checked to enable spanning tree protocol on the overlay bridge to avoid potential bridge loops. Only clear this box if this port group is free of any bridge loops, and you do not wish to run STP. One example is if this port group is connected to a Cisco switch running BPDU guard. A recommended alternative is to configure the port group with only a single port and use routed traffic only mode to make bridge loops impossible.
- d) **Routed traffic only** – Check this box to permit only routed bypass traffic. You must also configure an overlay IP address. Local protected devices should use this overlay IP as a gateway (either their default gateway or a static route) or Source NAT to allow incoming connections. Typically, you check Routed traffic only, unless you specifically need to bridge traffic. For example, if you have IP addresses in the same subnet on both sides of the tunnel, you are bridging traffic, so clear this box.

This setting prevents inadvertently carrying broadcast and multicast traffic sent by protected devices and can improve performance by using only a single port in the port group.

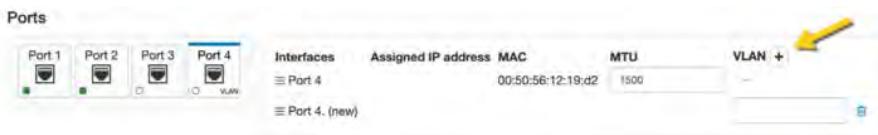
7. If you are connecting this port group to a router connected to a larger overlay network, you can configure static routes or even a default gateway.

8. Select **Update Settings**.

Add Interfaces to a Port

Each physical or logical port on an Airwall Gateway has a single interface by default, that can be assigned to a port group. If you are connecting an Airwall Gateway port to a switch using an 802.1q trunk allowing multiple VLANs, you need to add additional interfaces. To do this:

1. Up above the **Port Groups** section, select the **Port** and then click **Edit Settings**.
2. Next to **VLAN**, click the **+** to add a new VLAN for this overlay.
3. Enter the VLAN tag to match the VLAN config on the switch.



Do I need a gateway?

You only need a gateway if the Airwall Gateway needs to know how to reach additional networks from this port. The Airwall Gateway is the gateway for its protected devices. In general, using static routes (for example, 10.0.0.0/8) for your corporate network is preferable to using a default gateway (which is a 0.0.0.0/0 route), particularly if you have a bypass destination of 0.0.0.0/0 set up, since that will cause a conflict.

Set an Overlay to Automatically Manage Relay Rules

You can easily manage the relay rules for an overlay by setting it to automatically create relay rules that allow the trust relationships in the overlay.

Supported Versions

Conductor 2.2.10 and later

Required Roles

System administrators

Network administrators with permissions to the overlay



Note: You must first set up an Airwall Relay before you can enable automatic relay rules.

You can also configure Airwall Relay rules manually. See [Configure Airwall Relay rules](#) on page 81.

1. Open the overlay you want to automatically manage your relay rules.
2. Under **Info** on the right sidebar, select **Edit Settings**.
3. On the **General** tab, enable the **Manage a relay rule based on this overlay network's configuration** option.
4. Choose the Airwall Relays or Airwall Relay groups that you want this overlay to use.
5. Select **Save**.

The overlay creates relay rules that allow communication between all Airwall Edge Services in the overlay. Note that you still need to set up device to device trust for them to communicate.



Note: Airwall Edge Services try to connect directly first, and only use the relay if they cannot connect directly.



Note: Managed relay rules do not normally display on the **Airwalls** page. If you want to see them, you can go to **Airwalls > Airwall relay rules** and at the bottom right, check **Display system relay rules**.

Configure Device Trust

Configure device trust to set up secure communication between devices in your Airwall secure network.

To add trust between devices, you create or edit an Overlay network, and add the Airwall Edge Services that protect the devices you want to connect.

From **Overlays**, create or select the Overlay network for which you want to add trust.

You can see and add trust visually, or using the list of Devices.



Note: The default **Devices** tab list view does not show device trust relationships until you select a specific device or group. If trust has been configured for the selected device or group, your selected device or group is highlighted in blue, and the devices and groups it trusts are highlighted in a lighter blue.

In Advanced view:

- The **Visualization** tab shows trust relationships and allows you to add and remove trust visually.
- The **Devices** tab shows the list of devices and device groups in the Overlay, and allows you to add and remove trust.

Add and remove device trust

Set communication policies by adding trust between devices and device groups. You can use drag and drop to add and remove trust visually, or add trust on the Devices tab.

Supported Roles

System administrator

Network administrator who is a manager of the overlay.

Supported Versions

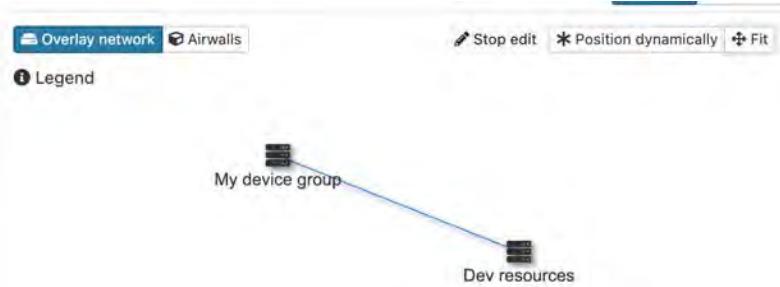
Drag and drop trust is available for v3.0 and later

You are configuring trust only between your primary device or group and each additional device and group respectively. This setting does not configure trust between all devices selected. Devices highlighted in gray trust only the primary device. Trust between the gray devices and groups must be configured separately. For a detailed example configuration and steps to set it up, see [Example: Complex device trust](#) on page 363

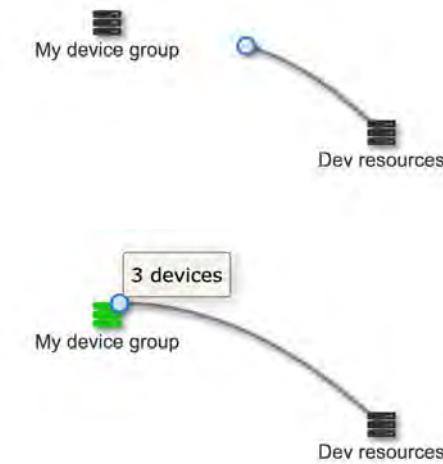
Add and remove device trust using drag-and-drop

1. Go to **Overlays** and select the Overlay network for which you want to set up trust.
2. If you are in the **Advanced view**, go to the **Visualization** tab.
3. To see the trust for a device or device group, select a device on the graph.

4. To add trust between devices and device groups:
 - a) Select **Edit mode** in the upper right of the visual network display.
 - b) If needed, select **Position dynamically** or **Fit** to arrange the devices and device groups so you can see them.



- c) Click and hold one device or device group, and drag a line to another to establish trust.



5. Continue dragging and dropping to add trust as needed on the overlay network.
6. **To remove trust** – In Edit mode, click the line between the devices you no longer want to have trust. When the line turns red, click to remove it:



Tip: If you right-click a device or trust line on the graph, you get a context menu where you can quickly add or remove trust between a device and all other devices in the network.

7. To leave Edit mode, select **Stop edit**.

For help in the graph, select **Legend** at the top left of the graph to show what you can do on the graph.

Add and remove device trust from the Devices tab

1. Go to **Overlays** and select the Overlay network for which you want to add trust.

2. On the **Devices** tab, click the Device name of the device or device group that you want to add trust for. The line will be highlighted in blue.
3. To establish trust with other devices or device groups, click the radio buttons next to them. The line will be highlighted in light blue/gray and you receive a message in the upper right of your screen that trust has been established. The following image shows trust between the Internet Access DMZ device and the other two devices.

Trust	Device name
<input type="radio"/> <input checked="" type="radio"/>	Device-126.1.40
<input type="radio"/> <input checked="" type="radio"/>	Device-126.9.80
<input checked="" type="radio"/>	Internet Access DMZ

Compare to this image, when you select one of the devices, the other device is not highlighted, which indicates the devices do not trust each other - they both only trust the Internet Access DMZ device. This is a hub-and-spoke arrangement.

Trust	Device name
<input type="radio"/>	Device-126.1.40
<input checked="" type="radio"/>	Device-126.9.80
<input type="radio"/> <input checked="" type="radio"/>	Internet Access DMZ

4. **To remove trust**, click the radio button again to remove it from the trust policy.
5. If you want to add a device group, but block certain devices in that group from the trust relationship, set trust for the group, and then use the toggle button next to the radio button to block trust with that device.

North Complex

Trust	Device name	Overlay IP	MAC address	Airwall
<input type="radio"/> <input checked="" type="radio"/>	Building 1	G2		
<input checked="" type="radio"/>	Building 2	G2		
<input checked="" type="radio"/>	TC Airwall-iOS		<input type="radio"/> NAT	TC Airwall-iOS
<input type="radio"/>	WW Android Agent		<input type="radio"/> NAT	WW Android Agent

6. You can see the trust relationships on the left. (In the Advanced view, go to the **Visualization** tab.)

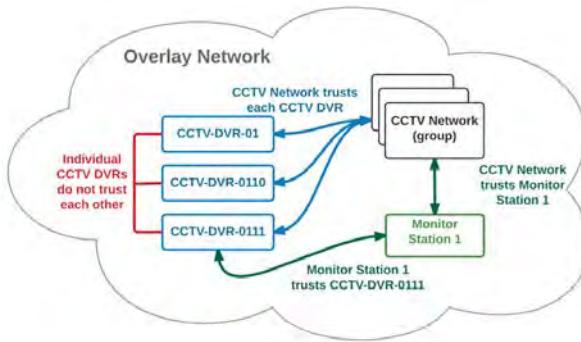
North Complex

Devices	Visualization	Timeline	Airwalls	Enabled	Disabled
<input type="checkbox"/> Overlay network	<input type="checkbox"/> Airwalls			<input type="checkbox"/> Save positions	<input checked="" type="checkbox"/> Restore positions
				<input type="checkbox"/> Refresh	<input type="checkbox"/> Fit



Example: Complex device trust

The example below shows a configuration in CCTV network that has multiple trust policies configured.



This example highlights a key concept to keep in mind when configuring device trust: you are only allowing trust between the initial device selected, highlighted in blue, and each individual device, highlighted in gray. Configuring trust between individual devices in gray is a separate step, as shown below.

1. First, configure the trust relationships for the CCTV Network device group.
 - a) In the **Devices** tab, click the button for **CCTV NETWORK**
 - b) Click the button for device group **CCTV-DVR-0110**
 - c) Click the button for device **CCTV-DVR-0111**
 - d) Click the button for device **CCTV-DVR-01**
 - e) Click the button for device **Monitor Station 1**

Trust	Device name	IP address	MAC address	Airwall
<input type="radio"/>	192.168.4.44	<input type="radio"/> 192.168.4.44	08:00:27:5f:3b:4b	HIP - 11
CCTV NETWORK □ 447				
<input checked="" type="radio"/>	CCTV-DVR-01	<input type="radio"/> 172.16.1.2	08:00:21:1a:be:69	HIP-3
<input checked="" type="radio"/>	CCTV-DVR-0110	<input type="radio"/> 11.11.11.150	08:00:27:e2:ae:17	HIP-7
<input checked="" type="radio"/>	CCTV-DVR-0111	<input type="radio"/> 11.11.11.151	08:00:27:e2:ae:18	HIP-7
<input checked="" type="radio"/>	Monitor Station 1	<input type="radio"/> 192.168.1.22	08:00:27:cf:4c:b3	HIP - 11

2. Next configure the additional trust required between Monitor Station 1 and CCTV-DVR-0111.
 - a) In the **Devices** tab, click the button for **CCTV-DVR-0111**. Note that the **CCTV NETWORK** device is automatically highlighted in gray, because trust between the two was already configured in step one.
 - b) Click the button for **CCTV-DVR-0111** to add it to the policy.

Trust	Device name	IP address	MAC address	Airwall
<input type="radio"/>	192.168.4.44	<input type="radio"/> 192.168.4.44	08:00:27:5f:3b:4b	HIP - 11
<input checked="" type="radio"/>	CCTV NETWORK □ 447			
<input checked="" type="radio"/>	CCTV-DVR-01	<input type="radio"/> 172.16.1.2	08:00:21:1a:be:69	HIP-3
<input checked="" type="radio"/>	CCTV-DVR-0110	<input type="radio"/> 11.11.11.150	08:00:27:e2:ae:17	HIP-7
<input checked="" type="radio"/>	CCTV-DVR-0111	<input type="radio"/> 11.11.11.151	08:00:27:e2:ae:18	HIP-7
<input checked="" type="radio"/>	Monitor Station 1	<input type="radio"/> 192.168.1.22	08:00:27:cf:4c:b3	HIP - 11

3. Refresh the screen to return to the default **Devices** view.

Configure Large scale device trust behind an Airwall Gateway

If you have an advanced configuration with a large number of devices that are one or more hops away behind a single Airwall Edge Service, you can use a special type of device with a 0.0.0.0 IP address. A 0.0.0.0 device effectively

functions as a wildcard, and when configuring trust, selecting the 0.0.0.0 device effectively applies the trust policy to all devices behind the parent Airwall Edge Service.



CAUTION: If you use the 0.0.0.0 device type, your Overlay network cannot use subnet routing or NAT, since each overlay network can only have one 0.0.0.0 address.

To create the 0.0.0.0 device and use it for trust configuration

1. Go to **Airwalls** and select an Airwall Edge Service.
2. Add a new device with the IP address set to 0.0.0.0. See [Add devices to the Conductor](#) on page 351 for more information about adding devices.
3. Go to **Overlays** and select the overlay network for which you are configuring trust.
4. On the **Devices** tab, click the button for the 0.0.0.0 device, and then select the other devices and groups in the overlay network that require communications with the devices represented by the 0.0.0.0 wildcard device.

See the Trust Relationships in an Overlay network

You can see and change trust relationships visually for an overlay on its page.

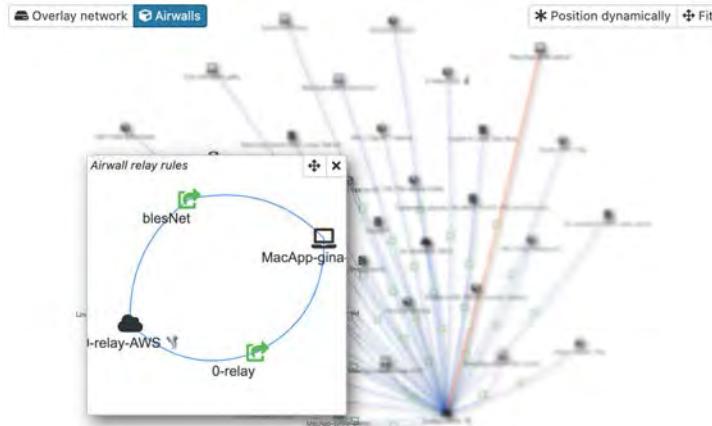
For how to edit trust relationships, see [Add and remove device trust](#) on page 360.

1. Go to **Overlays** and select the Overlay network for which you want to see trust.
2. If you are in the Advanced view, go to the **Visualization** tab.
3. Trust relationships are shown as lines drawn between devices and device groups. On this page you can:
 - **See the trust for a device or device group** – Select a device or device group, and its trust relationships are highlighted. In the simplified view, they also are highlighted on the device trust list on the right.
 - **Rearrange devices** – Select **Position dynamically** or **Fit** to automatically rearrange the visualization. Or, click and drag a device or device group to reposition it.



Note: In Edit mode, click and drag adds trust.

- **See the communication pathways and relays** – Select Airwalls to see how Airwall Edge Services are connected and the relays used in the overlay network



Set up Cloud Providers

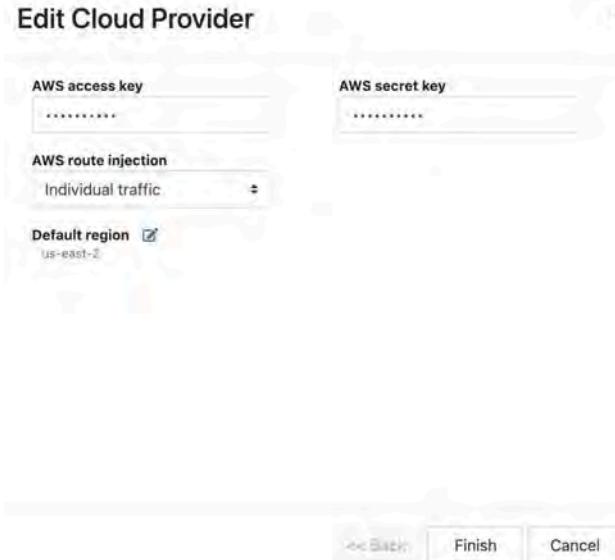
Setting up one of the supported cloud providers in your Conductor makes it easier to deploy Airwall Gateways and High-Availability Conductors directly from your Conductor.

Set up Amazon Web Services (AWS) as a cloud provider

Set up AWS as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

Set up AWS as a cloud provider

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page.
2. Select the **Cloud providers** tab and click **+ Add Cloud Providers**
3. In the **Add Cloud Provider** dialog, select the check-mark to the right of **Amazon Web Services** and click **Next**
4. Enter your **AWS access key**, **AWS secret key**, and **Default region**



5. The **AWS route injection** setting determines how new routes are added to the AWS routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:
 - If you are using a Airwall Relay, set to **Disabled**.
 - If you want to handle traffic for devices individually, set to **Individual traffic**.
 - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.



Note: All traffic is effectively ‘full tunnel’ mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

6. Click **Finish**

Your AWS cloud provider is displayed in the **Configured Cloud Providers** list.

Configured Cloud Providers	
Create Cloud HIPService + Add Cloud Provider...	
Amazon Web Services	
AWS route injection	Disabled
Default region	us-west-1
HIPservice templates +	
Name	Details
<input type="text"/>	

Set up Microsoft Azure as a cloud provider

Set up Microsoft Azure as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

Create an Azure Application to connect to the Airwall Conductor

Check your Azure documentation for the most recent instructions on creating an application.

1. In Azure, in **Active directory**, under **App registrations**, register or choose an application to act as Airwall API endpoint.
2. In the Azure application, in Certificates & secrets, create a new client secret for the app to connect to Conductor. Copy it to a secure location.



Important: You must copy the new client secret value at this step, because you won't be able to retrieve the key later.

3. From the Azure application you created, note the following information:
 - Azure **Application ID** – Get from the Azure application Overview page.
 - Azure **Application key** – The client secret you noted above.
 - Azure **Subscription ID** – In Azure, under **Users**, get the subscription details to find the ID. It's also at the top of your **Powershell** window.
 - Directory ID – Get **Directory (tenant) ID** from the Azure application Overview page.

The screenshot shows the Microsoft Azure portal interface. The user is navigating through the 'Azure Active Directory' section, specifically the 'App registrations' area. A specific application named 'AW Conductor' is selected. The application details pane shows the following information:

- Display name: AW Conductor
- Application (client) ID: 424362c6-28b4-4daf-b6aa-78311ce2354c
- Directory (tenant) ID: af23190-9801-4fed-94fa-dfe2e44a1ad0
- Object ID: 48dcf207-307a-4773-90ed-14ef13be2c1
- Supported account types: My organization only
- Redirect URIs: Add a Redirect URI
- Application ID URI: Add an Application ID URI
- Managed application in ...: AW Conductor

4. Set up a role for the application you created to use as authorization to create Airwall Gateways in your Azure environment.
 - a) From **Subscriptions**, select your subscription, and then select **Access control (IAM)**.
 - b) Add a role assignment, and assign the App you created to the role: For **Role**, select **Contributor**, and for **Assign access to**, select **User, group, or service principal**, and then search for your App. You can also select a custom role with the permissions you want. For more information, see Azure help: [Create a role in the Azure portal](#).

Add an Azure Cloud Airwall Gateway

You must [Set up Microsoft Azure as a cloud provider](#) on page 365 before you can add an Airwall Gateway in the Conductor

1. On the Airwalls page, (or in Conductor Settings Cloud providers tab), select **New cloud Airwall**, and then select **Microsoft Azure Airwall**.

The screenshot shows the Conductor interface with the 'Create cloud Airwall' button highlighted. A dropdown menu lists several cloud provider options:

- Alibaba Cloud Airwall
- Amazon Web Services Airwall
- Microsoft Azure Airwall
- Google Cloud Airwall

2. In v2.2.8 and later, select **Create stand-alone Airwall gateway**, and then **Next**.

3. In v2.2.8 and later, if you want to use a template to create the Airwall Gateway, select the template, select **Next**, and then give the Airwall Gateway a descriptive name. You can then skip to the next step.

To continue without a template and enter the information manually, just select **Next**.

- a) If you are filling in information manually, or want to change the template, fill in the **Name** and **Image and network options** for this Airwall Gateway. For **Machine type**, the default typically works. You can select a different size if needed for your purposes.

- b) Under **Airwall gateway image ID**, pick the Airwall Gateway image you want to use. The list shows the Airwall Gateway images available on your cloud provider.
- c) If you don't have a pre-configured virtual network, you need to create a new network. Click **Create new network** and fill in the form:
- **Network CIDR** – Enter an available network address and subnet mask in CIDR notation.
 - **Public subnet CIDR** – Must be a subnet of the main network. Traffic flows between the underlay interface of the Airwall Gateway and the Public IP address object in Azure.
 - **Protected subnet CIDR** – Must be a subnet of the main network. Traffic must pass through the Airwall Gateway or through manually-crafted routes.

When you're finished entering the information, select **Create network**, and when processing is complete, select **Back**.

Create Azure Airwall

Create new network (VPC)

Network name
test-net

Network options

Network CIDR 192.168.0.0/16	Availability zone eu-central-1b
Public subnet CIDR 192.168.1.0/24	Protected subnet CIDR 192.168.2.0/24

Create network

<< Back Cancel

- d) Back on the **Create cloud Airwall** page, select the network and public and protected subnets you just created.
4. Check the summary and if everything is correct, select **Create cloud Airwall**.
 5. Select **Finish**. It may take up to 5 minutes for Microsoft Azure to complete creating the Airwall Gateway.

You've completed creating an Azure cloud Airwall Gateway, and now need to configure Provision, License, and configure it. For help, see [Provision and License Airwall Edge Services](#) on page 161 and [Configure Airwall Edge Service Settings](#) on page 304.

Add Azure as a Cloud Provider in Conductor

1. In Conductor **Settings**, open the **Cloud providers** tab.
2. Under **Configured cloud providers**, click **Add cloud provider**, and then select **MS Azure**.
3. Fill in the form, using the values noted when creating an application in Azure:
 - **Application ID** – Enter the Azure **Application ID**.
 - **Client secret** – Enter the Azure **Application key**.
 - **Subscription ID** – Enter the Azure **Subscription ID**.
 - **Tenant ID** – Enter the **Directory (tenant) ID**.
4. The **Azure route injection** setting determines how new routes are added to the Azure routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:
 - If you are using a Airwall Relay, set to **Disabled**.
 - If you want to handle traffic for devices individually, set to **Individual traffic**.
 - If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.



Note: All traffic is effectively ‘full tunnel’ mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

- For **Default region**, click the **Sync** icon to check the connection and fill in your options. When it connects, select your default region from the list.

Edit Cloud Provider

Application ID 4243d2c6-28ba-4daf-b6aa-71	Tenant ID
Subscription ID 7e1fd3a2-f5b7-49ca-8416-ct	Application key
Azure route injection Individual traffic	
Default region  northeurope	

[<< Back](#) [Finish](#) [Cancel](#)

- Click **Finish**.

You're now ready to create cloud Airwall Gateways in Azure in the Conductor.

Set up Google Cloud as a cloud provider

Set up Google Cloud Platform as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

Set up Google Cloud as a cloud provider

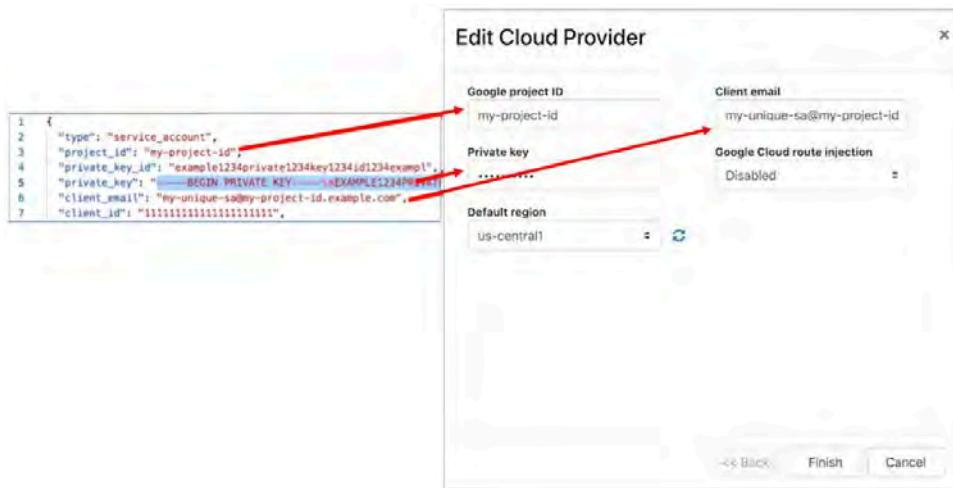
- Download a JSON key from your Google Cloud account. For assistance, see Google Cloud help: <https://cloud.google.com/iam/docs/creating-managing-service-account-keys>.



Note: Save the key file somewhere you can access it easily. You will need the information in this file when configuring the Google Cloud provider in the Conductor.

- Log in to your Conductor, and click the gear icon in the upper right to open **Settings**.
- On the **Cloud providers** tab, select **Add cloud provider**.
- Select **Google Cloud**, and then **Next**.

5. Fill in the **Google project ID**, **Client email**, and **Private key** fields with the corresponding information from the key file you downloaded.



6. The **Google Cloud route injection** setting determines how new routes are added to the Google Cloud routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

- If you are using a Airwall Relay, set to **Disabled**.
- If you want to handle traffic for devices individually, set to **Individual traffic**.
- If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.



Note: All traffic is effectively ‘full tunnel’ mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

7. Click **Finish**.



Note: If you need more information about Google Cloud Service Accounts, see <https://cloud.google.com/iam/docs/creating-managing-service-accounts>.

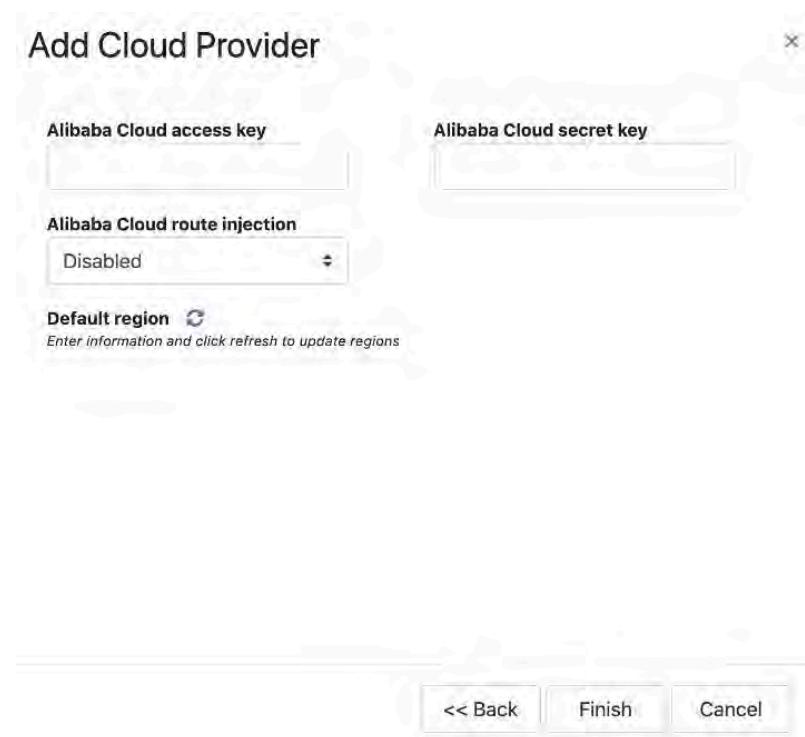
Set up Alibaba Cloud as a cloud provider

Set up Alibaba Cloud as a cloud provider in your Conductor to make deploying cloud Airwall Gateways and High-availability standby Conductor easier.

Set up Alibaba Cloud as a cloud provider

1. In the Conductor, select the gear icon in the upper-right to access the **Settings** page.
2. Select the **Cloud providers** tab and click **+ Add Cloud Providers**.
3. In the **Add Cloud Providers** dialog, select the check-mark to the right of **Alibaba Cloud** and click **Next**

4. Enter your **Alibaba Cloud access** and **secret keys**, and choose an option for **Alibaba Cloud route injection**.



5. The **Alibaba Cloud route injection** setting determines how new routes are added to the Alibaba Cloud routing table. The routes are for traffic on your protected overlay network between protected devices and the Airwall Gateway. Here are the recommended settings depending on your deployment details:

- If you are using a Airwall Relay, set to **Disabled**.
- If you want to handle traffic for devices individually, set to **Individual traffic**.
- If you want one route to send all traffic to the overlay port on the Airwall Gateway, set to **All traffic**.



Note: All traffic is effectively ‘full tunnel’ mode. With Individual traffic, you could add routes that send traffic around the Airwall Gateway.

6. By **Default region**, select the Refresh icon to get the list of regions from the provider, and then select your default region.
7. Click **Finish**

Your Alibaba Cloud provider is displayed in the **Configured Cloud Providers** list.

Alibaba Cloud		Actions
Alibaba Cloud route injection	Disabled	
Default region	us-east-1	
Airwall templates		+
Name	Details	
airwall-default	/ ecs.c5.large / vpc-0xli056muid19h6d1ms0v	

Integrate Third-party Services

How to integrate the Airwall Solution with third-party services.

Integrate Third-party Authentication with OpenID Connect

You can integrate a third-party authentication provider with person authentication in the Conductor using OpenID Connect (OIDC). If your users are already configured for single sign-on (SSO) with a third party, or if you have a large number of users, this integration streamlines your user management.



Note: You can only configure one OpenID Connect provider on the Conductor at a time. If you need to support many OIDC authentication providers simultaneously, you can choose providers that support federated login so you can connect to one provider and have that provider connect to other providers to authenticate users.



Important: To use OpenID Connect on macOS or iOS Airwall Agents, you must have a public certificate on your Conductor.

User Roles

In the Airwall Conductor, you configure person roles in OIDC by including them in groups. The OIDC group names are pre-configured in the Conductor, so when you make a person a member of one of the OIDC groups in the OIDC provider, they are automatically given that role in the Conductor. For instance, you can declare that all members of the OIDC provider's `cond_system_admins` group are system administrators in the Conductor, and that members of the OIDC `cond_remote_users` group are remote-access users.

Multi-factor Authentication

If your OIDC provider supports a multi-factor authentication (MFA) protocols, you can use MFA on your provider to require MFA for logging into your Conductor or for Airwall Agent session authentication.

Integrate Authentication with the Conductor

To successfully integrate authentication, you must

1. [Create and configure an application in your authentication provider](#).
2. [Configure OIDC on the Conductor](#).
3. [Set up Airwall Agents](#).
4. [Verify third-party authentication is working](#) on page 218

Since each provider is different, refer to the basics required here, and then the [Provider-specific instructions](#) that follow for integrating with some popular providers that support OIDC.

1. Create and configure an application in your authentication provider

Create and configure the application in your provider using the [Provider-specific Instructions](#) on page 210 before connecting it to the Airwall Conductor. Each provider's workflow is different, but here are the general steps:

1. Create an OpenID Connect application.
2. Configure it with the following information:

Field	Enter
Name	Whatever you want. For example, "Airwall Conductor"
Login Redirect URI	Your Conductor URI followed by <code>/user/auth/openid_connect/callback</code> . For example: <code>https://conductor.mycompany.com/user/auth/openid_connect/callback</code> . Note – If your Conductor is HA paired, add a second login redirect URI, with the same path added.

Logout Redirect URI	Your Conductor URI: https://conductor.mycompany.com
---------------------	---

3. Depending on your provider, set the authentication method to **basic**, or indicate you are using an **authorization code** for authentication (not a refresh token).
4. Allow the **groups** claim for grant. The **groups** claim is what allows the Conductor to match a user's group with what role they are given. Because **groups** is not a default OIDC claim, it must be turned on in the provider. For more details, see the [Provider-specific instructions](#).
5. Create four groups: `cond_system_admins`, `cond_READONLY_admins`, `cond_NETWORK_admins`, and `cond_REMOTE_users` to indicate the four different Conductor roles.
6. Add users to each group so they are assigned the correct role when logging into Conductor.
7. Give your users access to the application you created in your provider.
8. If you want to require MFA to log in, set it up in the OIDC provider. Generally MFA is associated with the app. Please consult your provider documentation for detailed instructions on setting up MFA.

2. Configure OIDC on the Airwall Conductor

1. Go to Conductor **Settings**.
2. Next to **Authentication**, select **Add provider**.
3. Select **OpenID Connect** and then select **Next**.
4. On the **Add Authentication Provider** page, under **General settings**, configure the Provider settings as follows (see the [Provider-specific Instructions](#) for help in finding this information):

For this Setting	Enter
Provider Name	Give your provider a descriptive name. This name appears as an option when logging into the Conductor.
Conductor host	Host of your Conductor. Must be in the format <code>https://conductor.mycompany.com</code> (no trailing slash)
OpenID Connect host	Must be in the format <code>https://hostname.com: {optional port}</code>
Issuer	Issuer provided by your OIDC provider. Sometimes this value is the same as the OpenID Connect host depending on the provider.
Client ID (sometimes called Identifier)	Token provided by your OIDC provider associated with the provider application
Secret	Secret token that goes with the Client ID

5. For **HA-paired Conductor host**, enter the Host of your HA Conductor (if applicable).
6. Configure the **Group** settings as follows, and then click **Next**:

For this Setting	Enter
Use groups to manage roles	Checked
System admin groups	Comma-separated list of groups from your provider that will give your user this role.
Read-only admin groups	Comma-separated list of groups from your provider that will give your user this role.
Network admin groups	Comma-separated list of groups from your provider that will give your user this role.

For this Setting	Enter
Remote-access user groups	Comma-separated list of groups from your provider that will give your user this role.

 **Note:** If users are in groups that match more than one of the roles, they are given the highest level of access possible (system admin, read-only admin, network admin, then remote-access user).

7. Configure any Group filters you want, and click **Finish**.
8. If you have non-public DNS servers configured in the Conductor under **Global Airwall Agent/client settings**, your users won't be able to reach the public addresses on their devices that include the OpenID Connect providers. You may need to configure DNS servers on the Conductor to add your OpenID Connect provider's DNS server.
9. After changing OIDC configuration, you need to log out and log back in to the Conductor to restart it. When you log back in, you can now choose your third-party authentication provider.

3. Set up the Airwall Agents

Any Airwall Agents authenticating using your third-party provider also need to be set up:

1. [Provision and License Airwall Edge Services](#) on page 161 in the Conductor.
2. Go to the **Overlays** page, scroll down to **People**, and click **Update**, and add the Airwall Agent as a member.
3. Also check that:
 - a) Airwall Agents are included in your Airwall Relay rules.
 - b) Airwall Agent devices have been added to the appropriate Overlays, and you've set device trust on the Overlays as needed.

Your users should now be able to log in using the third-party authentication provider.

Require third-party authentication

You can also require users to authenticate using the third-party provider either individually or as a group (in 2.2.3 and later Conductors). On the agent's **Airwall Agent** tab, or on a **People Group Properties** tab:

- Check the **Require Authenticated Airwall Session** box.
- Under **Provider**, choose the third-party authentication provider you created.

Provider-specific Instructions

Here are specific instructions for a few of the common third-party authentication providers. Note your provider's documentation may be more up-to-date.

Okta - Create Application and Set Up Group Claims

Create an Application

1. In Okta, go to **Applications**.
2. Select **Add Application**.
3. Under **Create New Application**, select **Web**.
4. Set **Allowed grant type** to **Authorization code**.
5. Set the **OpenID Connect host** to the same value as the **Issuer** in Conductor. This value is found on the under **OpenID Connect ID Token** on the **Sign on** tab.
6. Note the Client ID and Secret that are in your application, on the **General** tab under **Client Credentials**.
7. Set up Groups Claim (see below).

Set up Groups Claim

To set up Okta to allow the groups claim in OpenID Connect, use the Classic UI.

1. In Okta Authentication, go to **Security**, and select **API**.
2. From the **Authorization Servers** tab, open the default API (or whatever API you are assigning to your application).

3. On the **Scopes** tab:
 - a) Add a scope named `groups`.
 - b) Uncheck **Set as Default**.
 - c) Check **Include in Public Metadata**.
4. On the **Claims** tab:
 - a) Add a claim named `groups`.
 - b) Set **Include in token type** to **ID Token / Always**
 - c) Set **Value type** to **Groups**
 - d) Set a filter of **Matches regex** to `.*`. Alternatively, set a filter of **Starts with** and set to the prefix for your group names that you want to use in Conductor. For example, set **Starts with** to `cond_`.
 - e) Set **Include in** to **Any scope**.

OneLogin - Create Application

1. In OneLogin, select **Add App**, and then choose **OpenID Connect (OIDC)**.
2. Set **Authentication method** to **basic**.
3. Add users to the roles you want. For example, to make them a system admin, add them to **cond_sysadmins**.

 **Note:** In OneLogin, roles are mapped to OIDC groups (groups mean something else), so add users to roles, not groups.
4. In your OneLogin application, on the **Parameters** tab, configure the roles-to-groups mapping. Edit the groups and modify the default on the **Roles** field to: **User roles, --No transform--**.
5. Note the information you'll need to configure the Conductor:
 - a) **OpenID Connect host**: This is your OneLogin login URL, for example, `https://my-company.onelogin.com`.
 - b) **Issuer**: On the **SSO** tab, select **OpenID Provider Configuration Information** for the **Issuer**.
 - c) **Client ID and Secret**: These are both on the **SSO** tab.

Auth0 - Create Application

1. In Auth0, under **Applications**, select **Create Application**, and then **Regular Web Application**.
2. Skip the quick start.
3. On your new application's **Settings** page:
 - a) Change **Application Properties > Token Endpoint Authentication Method** to **Basic**.
 - b) In **Application URIs > Allowed Callback URLs**, add the login redirect URI. See the Login Redirect URI near the top of this page.
 - c) In **Application URIs > Allowed Logout URLs**, add the logout redirect URI. See the Logout Redirect URI near the top of this page.

 **Note:** Auth0 does not currently support OpenID Connect Logout.
- d) Note the following information in Auth0 that you'll need to configure the Conductor:
 - **Basic Information > Domain**: On the Conductor, you enter this information as **Open Connect host** and **Issuer** (note that the https is required).
 - **Basic Information > Client ID and Client Secret**: On the Conductor, you enter this information as Client ID and Secret.
- e) When finished, select **Save Changes** at the bottom of the **Settings** page.

4. Add the rule required by Auth0 to set OIDC groups. (In Auth0, roles map to groups on the Conductor.)
 - a) Under **Auth Pipeline > Rules**, select **Create Rule**.
 - b) Select **Empty Rule**.
 - c) Set the name to **Add groups to OIDC token**.
 - d) Add this rule:

```
function (user, context, callback) {  
    const namespace = 'https://<your issuer>';  
    const assignedRoles = (context.authorization || {}).roles;  
  
    let idTokenClaims = context.idToken || {};  
    let accessTokenClaims = context.accessToken || {};  
  
    idTokenClaims[` ${namespace}/groups`] = assignedRoles;  
    accessTokenClaims[` ${namespace}/groups`] = assignedRoles;  
  
    context.idToken = idTokenClaims;  
    context.accessToken = accessTokenClaims;  
  
    callback(null, user, context);  
}
```

- e) Change the namespace in the rule to be your Auth0 issuer. Example: <https://dev-abc123.auth0.com>
5. Following Auth0 instructions, add roles to users that give them the proper role in the Conductor.

Azure Active Directory - Create Application

Note that the Azure AD documentation may be more up-to-date and the settings in your Azure AD account may vary.

1. In Azure Active Directory (AD), select **App registrations**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the 'Microsoft Azure' logo and a search bar. Below the header, the text 'Default Directory | Azure Active Directory' is displayed. On the left side, there's a sidebar titled 'Manage' containing various options like 'Users', 'Groups', 'External Identities', etc. The 'App registrations' option is highlighted with a yellow arrow pointing to it.

- Overview
- Getting started
- Preview hub
- Diagnose and solve problems
- Manage
- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations** (arrow)
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names

2. Select **New Registration**, and fill in the form as follows:

- **Name** – Enter a name for the Application (for example, "Airwall Conductor").
- **Supported account types** – Select **Accounts in any organizational directory (Any Azure AD directory – multitenant)**.
- **Redirect URI** – Select **Web**, and then enter the URL of your Conductor followed by /user/auth/openid_connect/callback:

The screenshot shows the 'Register an application' form in the Microsoft Azure portal. The 'Name' field is filled with 'Airwall Conductor'. The 'Supported account types' section has the 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)' option selected. The 'Redirect URI (optional)' field contains 'https://airwall-rs.tempered.io/user/auth/openid_connect/callback'. A note at the bottom states: 'By proceeding, you agree to the Microsoft Platform Policies'.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Default Directory >

Register an application

* Name
The user-facing display name for this application (this can be changed later).
Airwall Conductor

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Default Directory only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only
Help me choose...

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web https://airwall-rs.tempered.io/user/auth/openid_connect/callback

By proceeding, you agree to the Microsoft Platform Policies

Register

3. Click **Register**. Take a note of the Application (client) ID and the Directory (tenant) ID provided by Azure AD.

Once you've registered the Application, Azure AD provides a set of IDs that you configure in the Conductor when you set up Azure AD as an OIDC provider. Here is how they map to the Edit Authentication Provider options in the Conductor:

The screenshot shows the 'Edit Authentication Provider' page in the Airwall Conductor interface. On the left, there's a sidebar with 'Overview', 'Quickstart', 'Integration assistant', 'Manage' (selected), 'Branding', and 'Authentication'. The main area has tabs for 'Essentials', 'General settings', and 'Provider name (optional)'. Under 'General settings', there are fields for 'Conductor host' (https://), 'OpenID Connect host' (https://sts.windows.net), 'Issuer' (https://sts.windows.net/8040...), 'Client ID' (0dfa8445-5500-4ee8-9cf2-f89a...), and 'Secret' (a masked password). Yellow arrows point from the 'Application (client) ID' and 'Directory (tenant) ID' fields in the 'Edit Authentication Provider' page to the 'Client ID' and 'Issuer' fields respectively. Another yellow arrow points from the 'Object ID' field to the 'Client ID' field.

- Application (client) ID – Enter in the **Client ID** box.
- Directory (tenant) ID – Append this ID to <https://sts.windows.net/> and enter in the **Issuer** box .

4. In Azure AD, create a Client Secret:

- a) Select **Certificates & secrets**.
- b) Select **New client secret**.

Airwall Conductor | Certificates & secrets

Certificates
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID
No client secrets have been created for this application.			

- c) Add a description, and select when the secret expires.

Add a client secret

Description

Expires
 In 1 year
 In 2 years
 Never

Add **Cancel**

- d) Select **Add**.

5. On the **Client secrets** page, copy the **Value** (not the ID). Enter the Value as the secret in the Conductor.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret	Description	Expires	Value	ID
Conductor Client Secret	Conductor Client Secret	12/31/2299	1RXR8b-JVzKowS2ZI41f9_p_1bm-k-3	eb780cff-a4ed-44d1-8a-97bae7f51bf7

Edit Authentication Provider

General settings

Provider and address	Conductor host
Azure AD	<input type="text" value="https://"/>

In your OpenID Connect provider, set the login redirect URL to https://airwall.conductorairwall.com/login/auth/oidc/conector/MSAuth. Set the logout redirect URL to https://airwall.conductorairwall.com/logout.

OpenID Connect host
Issuer

Client ID
Secret

Use OpenID Connect logout

6. From the newly registered application in Azure AD, select **Authentication**.

7. Under **Implicit grant**, verify that **Access tokens** is checked.

The screenshot shows the Azure portal's 'Authentication' configuration page for the 'Airwall Conductor' application. On the left, a navigation menu lists various settings like Overview, General, Integration assistant, and Authentication. The 'Authentication' option is selected. In the main pane, under the 'Web' section, there are fields for 'Redirect URIs' and 'Logout URL'. Below these, the 'Implicit grant' section is expanded, showing a note about it being recommended for single-page web applications. It includes a checkbox for 'Access tokens' which is checked, and another for 'ID tokens' which is unchecked. A yellow arrow points to the 'Access tokens' checkbox.

8. In the Azure AD application, set up the groups claim:
- From the menu on the left, select **Token configuration**.
 - Select Add groups claim.
 - Check all of the group types:

The screenshot shows the 'Edit groups claim' configuration page. At the top, a note says 'Adding the groups claim applies to Access, ID, and SAML token types. Learn more.' Below this, a section titled 'Select group types to include in Access, ID, and SAML tokens:' has four checkboxes: 'Security groups' (checked), 'Directory roles' (checked), 'All groups (includes distribution lists but not groups assigned to the application)' (checked), and 'Groups assigned to the application' (unchecked). At the bottom, a section titled 'Customize token properties by type' contains three expandable dropdowns: 'ID', 'Access', and 'SAML'.

- Under Customize token properties by type, expand and configure the properties as follows:
 - ID** – Select **sAMAccountName**.
 - Access** – Select **sAMAccountName**.
 - SAML** – This is not used.

9. In Azure AD, create the groups you want to use for the Conductor. Here are some suggested groups:

- cond_network_admins
- cond_READONLY_admins
- cond_REMOTE_users
- cond_SYSTEM_admins

The screenshot shows the 'Groups | All groups' page in the Microsoft Azure portal. On the left, there's a sidebar with options like 'All groups', 'Deleted groups', 'Diagnose and solve problems', 'Settings' (with 'General', 'Expiration', and 'Naming policy' sub-options), 'Activity', 'Privileged access groups (Preview)', and 'Access reviews'. The main area has a search bar and a 'Add filters' button. A note says 'This page includes previews available for your evaluation. View preview →'. Below is a table with four rows of group details:

Name	Object Id	Group type
cond_network_admins	414ec0b1-e7f4-4499-a830-98d...	Security
cond_READONLY_admins	d3921313-00d1-4391-8196-7...	Security
cond_REMOTE_users	cd12a46e-0d93-458c-b126-68...	Security
cond_SYSTEM_admins	7727f1de-6c61-42a0-813d-6a...	Security

10. Add users to Azure AD, and assign them to the appropriate groups for Conductor access:

The screenshot shows the 'Network Admin | Profile' page in the Microsoft Azure portal. On the left, there's a sidebar with options like 'Diagnose and solve problems', 'Manage' (with 'Profile', 'Assigned roles', 'Administrative units', 'Groups', 'Applications', 'Licenses', and 'Devices'), and 'Edit', 'Reset password', 'Revoke sessions', 'Delete', 'Refresh', and 'Got feedback?' buttons. The main area shows a user profile for 'netadmin@onmicrosoft.com' with a large orange 'NA' icon. It displays 'User signed in' and 'Group memberships: 1'. A yellow arrow points to the 'Group memberships' link. At the bottom, it shows 'Creation time: 12/15/2020, 1:02:52 PM'.

You are now ready to configure Azure AD as an OIDC provider in the Conductor as described in [2. Configure OIDC on the Airwall Conductor](#) on page 209. For the mappings from Azure AD to the Conductor, see steps 3 to 7 above.

Verify third-party authentication is working

To verify your configuration:

1. Log out of Conductor.
2. Open an incognito window and log in, choosing the provider name you chose in the Conductor.
3. Log in as a user you've set up with third-party provider. You should be able to log in to the Conductor using your third-party provider credentials.

To verify a client can connect:

- After the client logs in using the third-party provider, ping the client.

Troubleshooting Third-party Authentication User Login

If user login is failing with “Could not find that username/password combination,” verify:

- The user has been given access to your OIDC application in the third-party provider
- The user is a member of a group in your provider that is mapped to a user role in the Conductor
- The “groups” claim is allowed in your application in the provider
- The user typed in their username and password correctly

Check the Conductor log for additional clues for why the login failed. For instance, you may see a log message that a person does not match any groups to get a role.

Configure LDAP authentication on Conductor and Airwall Edge Services

You can use Active Directory and LDAP authentication with the Conductor to streamline user account management. When LDAP is configured, users can choose to log in with an LDAP account on the Conductor login page.

There are currently three different ways to authenticate with Conductor.

- With a Conductor account. These are local accounts that log directly into the device
- With LDAP authentication. This allows you to authenticate with any LDAP server, including Microsoft Active Directory services.
- With a third-party authentication provider that supports OpenID Connect. See [Integrate Third-party Authentication with OpenID Connect](#) on page 208.

To set up a LDAP authentication, you need to already have an LDAP server accessible to the Conductor.



Note: These instructions use Microsoft Active Directory, but other LDAP services also work.

There are four different roles in the Conductor:

- **System Administrator** – These users have full access to the Conductor and can adjust any settings. Note that to edit LDAP settings, you must be logged in locally to the Conductor, not through LDAP.
- **Read-only System Administrator** – These users have read access to the Conductor, but cannot make changes.
- **Network Administrator** – These users have access to and can adjust any overlay network they are a manager of. They do not have access to Conductor Settings.
- **Remote Access User** – These users can only see their own information, and can log in with their credentials if authentication is required for their Airwall Agent or Server.

For more detailed role information, see [Understand People Roles and Permissions](#) on page 49.

Step 1: Set up and configure your LDAP server

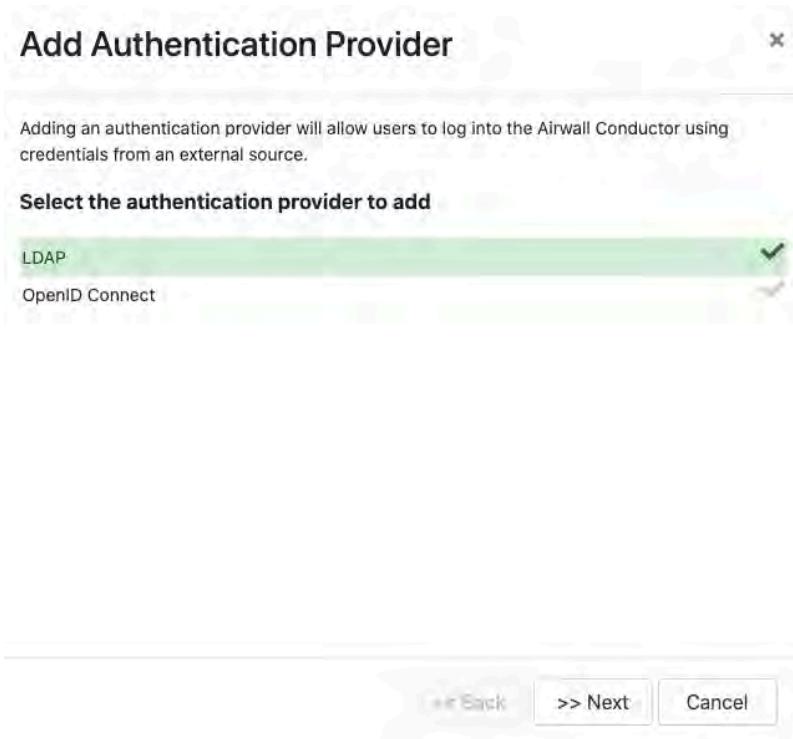
LDAP is not enabled in Active Directory by default, so you will have to turn it on. Once you have LDAP working and running, you can start.

Create a dedicated account with the necessary permissions to authenticate. In Active Directory, you could create a service account under the root "Users" OU, and make it a Domain Admin.

Step 2: Enter and verify your local Conductor admin account credentials, and select Authentication provider

1. Log into Conductor locally (not through LDAP) as a System Administrator. (Only local administrators have access to authentication provider settings.)
2. Open **Settings**, and next to **Authentication**, select **Add Provider**.

3. Select **LDAP** from the list of providers.



Step 3: Enter your LDAP settings

You will need to know the following values:

- Host (Hostname or IP address)
- Port (636 is the default)
- If you are using a dedicated LDAP service account, the fully-distinguished path for the user account, and the password

Under **LDAP host settings**, enter the information for your LDAP host, and select **Next**. For more details on these settings, see [LDAP host settings](#) on page 225.

Edit Authentication Provider

LDAP host settings

Host	Port
192.168.88.10	636
Bind DN <small>(leave blank for anonymous access)</small>	Password
cn=conductor LDAP, cn=users, dc=ldap.	*****
Connect method	SSL

Validate server certificate

Test connection

[<< Back](#) [>> Next](#) [Cancel](#)



Note: TLS LDAPS communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged.

Step 4: Configure Search Settings

This page can mostly be left as-is, unless you have special settings you wish to set. You can search for user accounts here to ensure that the Conductor can search the directory. Select **Next**. For more details on these settings, see [LDAP search settings](#) on page 226.

Edit Authentication Provider

LDAP search settings

Base search DN	User UID attribute
dc=serverpod,dc=net	sAMAccountName
Custom search filter	<small>Eg. (department=IT), (objectClass=person), etc</small>
(memberOf=CN=Developers@TempNetworks,OU=TempNetworks,OU=Host)	

Test LDAP search

tnw **Test LDAP search**

① Enter a user name and click the 'Test search' button to test searching for a user

[<< Back](#) [>> Next](#) [Cancel](#)

You can test the search by entering a search term and selecting **Test LDAP search**.

Step 5: Configure Group Settings

The Conductor assigns LDAP users to one of the four account types above by making them a member of a security group.

If you don't have appropriate groups already, create these groups in LDAP to link to Conductor roles (you can use different names – using cond_ makes it easier to see which roles are for the Conductor). By default, these groups place the users into the following roles:

- **cond_admin** – System Administrator
- **cond_READONLY** – Read-only System Administrator
- **cond_NETWORK** – Network Administrator
- **cond_REMOTE** – Remote Access User

Since users cannot have more than one role at a time, if they are members of multiple groups, they'll be assigned the role with the most permissions.

Remember to test the settings to ensure that Conductor can see all of the groups you reference on your LDAP server.

1. For **LDAP group settings**, enter the groups for the roles you want LDAP users to have, and **Group search attributes**, and select **Next**. For more details on these settings, see [LDAP group settings](#) on page 227.

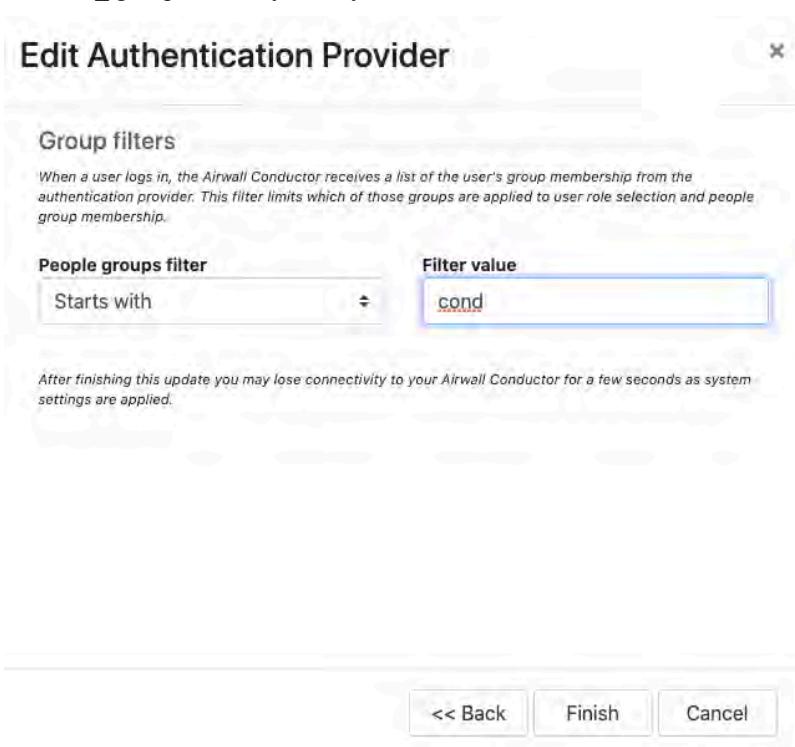
The screenshot shows the 'Edit Authentication Provider' dialog with the 'LDAP group settings' tab selected. The 'Enabled' button is highlighted. The 'Group search attributes' section contains 'Group class name: group' and 'Group attribute name: member'. Under 'LDAP group settings', there are four sections: 'System admin groups' (containing 'cond_admin'), 'Read-only admin groups' (containing 'cond_READONLY'), 'Network manager groups' (containing 'cond_NETWORK'), and 'Remote-access user groups' (containing 'cond_REMOTE'). A yellow box highlights the 'Test group settings' button at the bottom left. At the bottom right are buttons for '<< Back', '>> Next', and 'Cancel'.

You can also add other security groups to the configuration, separated by commas.



Note: You can set up these groups on your LDAP server after setting up LDAP on the Conductor, but **Test group settings** will fail.

- For **Group filters**, enter filters to specify which LDAP groups the Conductor sees. For example, if you've created the cond_groups above, you may want to set the filter to **Starts with** with a value of cond.



- Select **Finish**

You may lose connection briefly as the new settings are applied.

Step 6: Configure user onboarding

Configure user onboarding for the people groups created above to give users access to overlay networks through Airwall Agents and Servers. Setting the groups up beforehand simplifies user onboarding.

- In the Conductor, create **People groups** that match the LDAP groups you specified above (for example, cond-admin)
- Specify user onboarding options as you create the groups. For details, see [Set up a People Group](#) on page 74.

As users log in through LDAP, they are added to these **People groups** and given an activation code that activates the permissions and other options you specified for the **People groups**.

Step 7: Set up Conductor management access

You can also set up access for your Conductor system and network admins individually.

- 1. Add administrators to Overlays** – Add administrators individually as members of Overlay networks to give them access to the resources they need. You can add them from their **People** page, or from an Overlay page:

 - From the person's **People** page, next to **Overlay networks**, select **Edit**. Add the person as a member or manager of Overlays.

The screenshot shows the 'People - Local Administrator' page in the Conductor interface. On the left, there is a sidebar with various settings like 'User directory', 'Full name', 'Username', 'Role', etc. On the right, there are sections for 'Info' (with a note about no tags in use), 'People groups' (not a member of any people groups), and 'Overlay networks' (not a member of any overlay networks). A prominent 'Edit' button is located next to the 'Overlay networks' section.

Edit memberships

The screenshot shows a modal dialog titled 'Edit memberships'. It contains a table with two rows. The first row has 'Network' (Remote user network) and 'Member' (checkmark). The second row has 'Network' (Contractor network) and 'Member' (checkmark). At the bottom right of the dialog is a 'Close' button.

- From the **Overlays page**, open the overlay, and under **People**, select **Update**. Add the administrators as members or managers of the overlay.

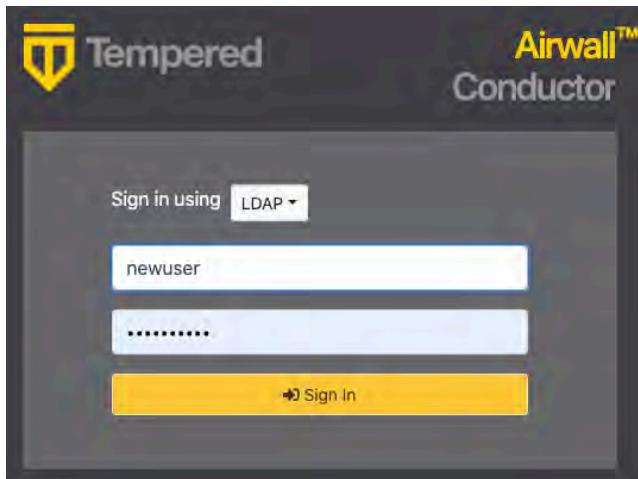
The screenshot shows the 'People' page with an 'Update' button. Below it, there are two entries: 'Sys Admin' and 'Manager'.

2. **Add administrators to People groups** – Similarly, you can add administrators to **People groups**, from their People page or add several administrators from the People group:
 - **From a person's People page** – Next to **People groups**, select **Edit** and select the **People groups** with the permissions they need.
 - **From a People group** – Open the **People group**, and on the **People** tab, select the people to add.

Step 8: Verify by logging in to the Conductor

Verify that LDAP is set up by logging in and checking permissions.

1. Log out from your local administrator account.
2. Next to **Sign in using**, select **LDAP**, and log into the Conductor with an LDAP account.



3. Check that permissions are set correctly for that user.

See also: [Configure user authentication for Airwall Agents and Airwall Servers](#) on page 204.

Mirror traffic from your Airwall Gateways to a packet analyzer tool

You can mirror traffic from your Airwall Gateways to allow common packet analyzer/visibility tools (like Nozomi or Wireshark) to see what's going on in your Airwall secure network.

Caution: Packet analysis is a notoriously risky activity for security. Parsing unknown, uncontrolled inputs for a wide range of protocols is error prone. When employing a packet analysis tools, it's best practice to segment off the packet processing into an isolated security sandbox.

Supported Versions

Conductor and Airwall Gateways v2.2.11 and later

Required Role

- System or network administrators
- Permissions to edit the Airwall Gateways used as the Mirror Destination and Sources. You need to be a manager of at least one overlay that these Airwall Gateways are in.

Supported on these Airwall Edge Services

Airwall Gateways: 2.2.11 hardware and virtual gateways:

- **For Mirror Destination:** *Production environments:* Recommend Airwall Gateway 300v or 500 only.
Testing: Airwall Gateway 75, 150, or 250.
- **For Mirror Source:** Any Airwall Gateway.

Bulk editing does not support this configuration.

Before you begin



CAUTION:

To allow a packet analyzer to view traffic on an Airwall secure network, port mirroring requires copying potentially-sensitive traffic and delivering a copy of it where your packet analyzer can access it. This additional copy can introduce a security risk and impact the performance of your network:

- **Security risk and impact** – A security risk is introduced in handling the copy of sensitive traffic that must also be secured.
- **Performance impact** – Mirroring traffic to a remote Airwall Gateway may incur up to a 3-5x performance penalty due to the overhead of processing additional copies of the traffic and fragmenting large packets. The more traffic you mirror, the higher the impact. See [Adjust performance for mirrored traffic](#) on page 394 for suggestions on mitigating the performance impact.

Requirements

To set up port mirroring, you need:

- A Packet Analysis Tool (such as Nozomi or Wireshark)
- The permissions listed under **Required Role** above.
- An Airwall Gateway to use as the Mirror Destination (see [Supported on these Airwall Gateways](#) for recommended models)
- One or more Airwall Gateways that you want to mirror the traffic on (to use as Mirror sources)



Note: If you are using GRE or ERSPAN source to packet analyzer, you can use an existing overlay port group. If you're using a Mirror Destination port group, the Mirror Destination Airwall Gateway needs a free port.

How does it work?

The following diagram shows how to set up port mirroring to avoid leaking sensitive network information.

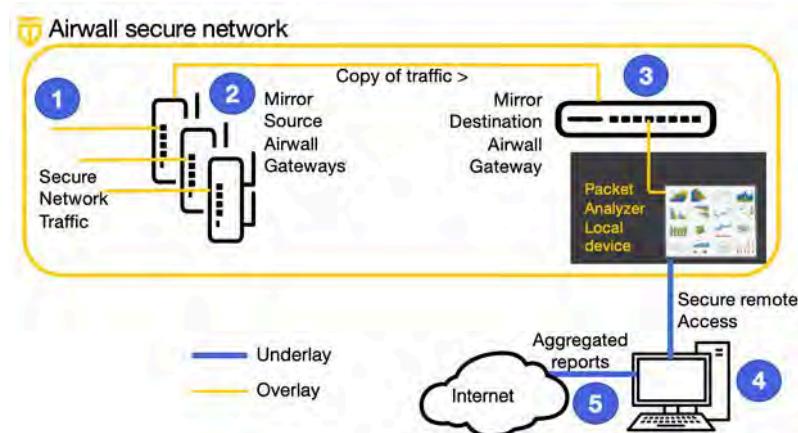


Diagram Flow:

1. Secure network traffic to and from the Mirror Source Airwall Gateways is collected.
2. Mirror Source Airwall Gateways send a copy of traffic data to the Mirror Destination Airwall Gateway.
3. Mirror Destination Airwall Gateway sends the data to the Local device for the Packet Analyzer.
4. Admin securely logs in to packet analyzer to access and analyze data and export reports.
5. Admin releases reports that aggregate the data.

For more ways to configure mirrored traffic, see [More Mirrored Traffic Scenarios](#) on page 399.

Choose how to mirror traffic

There are two ways you can set up the Mirror Destination Airwall Gateway, depending on how you are connecting your packet analyzer to it:

- **Local Device Destination** – The recommended way to mirror traffic is to send the traffic to a local device for your packet analyzer. See [Mirror Traffic to a Local Device destination \(Recommended Way\)](#). This method uses GRE or ERSPAN to send traffic to a local device for the packet analyzer on the Mirror Destination Airwall Gateway.
- **Mirror Destination Group** – You can also send mirrored traffic to a dedicated port group attached to a physical cable. See [Mirror traffic to a dedicated port](#) on page 400. This method uses a special type of port group (Mirror Destination group).

If you are using a Mirror Destination group, you can't use a physical or virtual switch without special configuration. This particularly impacts the Airwall Gateway 300v, since the hypervisor uses a virtual switch. You must either use a physical cable to directly connect the Airwall Gateway to the packet analyzer, or consult your switch vendor's documentation on how to configure it to carry mirrored traffic.

Mirror Traffic to a Local Device destination (Recommended Way)

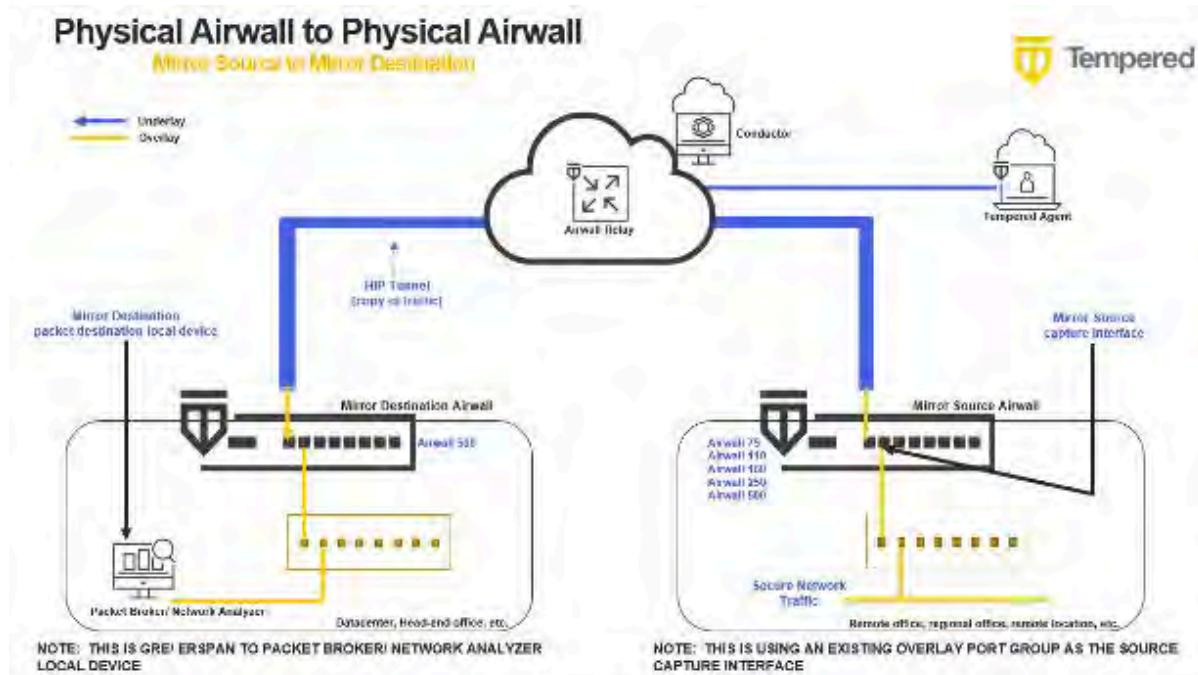
The recommended way to mirror traffic is to send the traffic to a local device for your packet analyzer.

To mirror traffic to a local device, you need to:

1. Create a local device for your packet analyzer tool.
2. Configure a Mirror Destination to send to a Local Device.
3. Configure Airwall Gateways to act as Mirror Sources.
4. Adjust performance for mirrored traffic.
5. Set up security for mirrored traffic.
6. Configure your packet analyzer tool.

These steps are described in more detail in the following sections.

Here is a diagram showing this scenario:

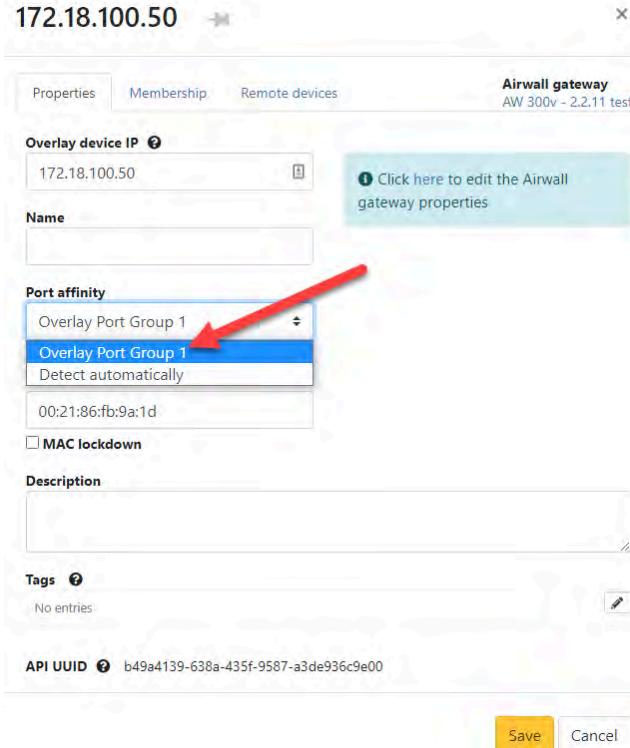


Create a local device for your packet analyzer tool

Create a local device on a dedicated overlay port group for your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information).

The destination for your mirrored traffic can be your packet analyzer set up as a local device on your Mirror Destination Airwall Gateway.

1. Add the packet analyzer tool as a local device to the Airwall Gateway that you're going to use as your Mirror Destination (the one that receives the mirrored traffic and sends it to the destination, which is your analyzer).
2. When you're adding the device (either manually or through auto-discovery), you must set Port affinity (it can't be left on auto).



For more information, see [Add devices to the Conductor](#) on page 351.

If you are using this method to connect your packet analyzer tool, you need to configure your mirror destination as described on this page: [Configure a Mirror Destination to send to a Local Device](#) on page 392

Configure a Mirror Destination to send to a Local Device

The Mirror Destination Airwall Gateway receives the mirrored traffic and sends it to your packet analyzer (or network analyzer or packet broker).

If your packet analyzer supports receiving packets encapsulated in GRE or ERSPAN, this is the preferred configuration. It avoids the possibility of mirrored traffic being recirculated on your network and the MAC address table issues with switches. It also provides additional fields to your packet analyzer that allow it to distinguish between traffic captured by multiple Airwall Gateways (using GRE key/ERSPAN session ID) and detect lost or reordered packets (using ERSPAN sequence number).

1. On the Airwall Gateway page, go to **Ports > Port mirroring**.
2. Select **Edit Settings**.
3. Next to **Configurations**, select the + to add a mirroring configuration.

4. In your new configuration:

- Set the **Enabled** toggle to On.



Note: After configuration, use this toggle to turn mirroring on and off.

- Under **Type**, select **Mirror Destination**.

- Under **Packet destination**, select the local device for your packet analyzer you set up earlier.



Note: The device will not show up as destination when you're selecting the Mirror Destination Airwall Gateway unless you've set a specific port group affinity (not Auto). See [Create a local device for your packet analyzer tool](#) on page 391.

- Under **Encapsulation type**, select the encapsulation (GRE or ERSPAN Type I, II, or III) supported by your packet analyzer. For example, for Nozomi, pick ERSPAN type II. Refer to documentation of your packet analyzer to determine which encapsulations it supports.



- Optional** – Enter any information allowed for the type you selected (for example, GRE key or session ID).
- Optional** – Under BPF filter, add any BPF filters you would like to use to filter the traffic that is mirrored to this Mirror Destination. See [BPF Settings for Port Mirroring](#) on page 396.



Note: If you use a BPF expression on the Mirror Destination, that's the default for all of the Mirror Sources, unless you set a BPF expression on the source, which overrides this default.

5. Select **Update Settings**.

You should be able to see some traffic from the Mirror Destination to the packet analyzer local device.

Configure Airwall Gateways to act as the Mirror Sources

You configure Mirror Source Airwall Gateways to send network information to the Mirror Destination Airwall Gateway.



CAUTION: If you capture traffic on all ports of the overlay port group, you may set up a loop. To avoid this, in your configuration set a BPF filter of “ip proto not 47” to exclude mirrored traffic. See [BPF Settings for Port Mirroring](#) on page 396.

If you use GRE Transparent Ethernet Bridging, ERSPAN type II or ERSPAN type III – You can use GRE key or Session ID to identify which source the packets arrived on.

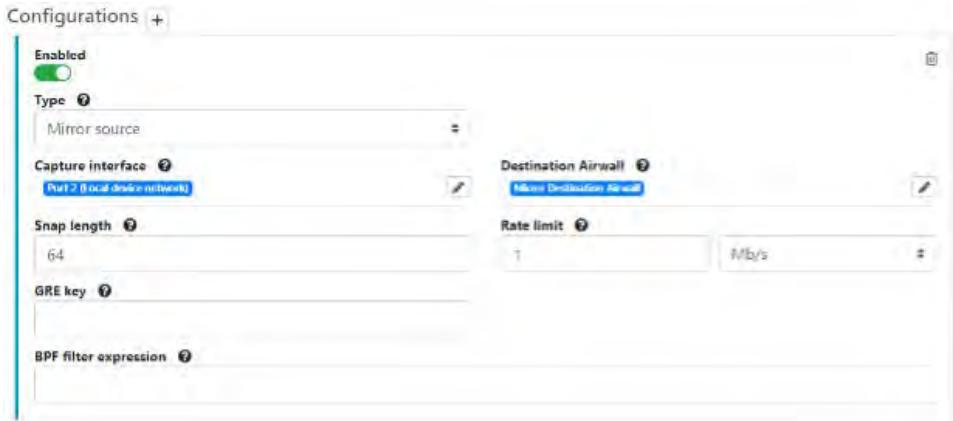


Note: You can set up the Mirror Destination to also be a Mirror Source, to include that Airwall Gateway's traffic in the information sent to the packet analyzer. In this case, be sure to set a BPF filter to exclude the mirrored traffic.

- On a Mirror Source Airwall Gateway, go to **Ports > Port mirroring**.
- Select **Edit Settings**.
- Next to **Configurations**, select the + to add a mirroring configuration.

4. In your new configuration:

- Under **Type**, select Mirror Source.
- Under **Destination Airwall**, select the Airwall Gateway you set up as the Mirror Destination.
- Under **Capture interface**, select the interface you want to capture network information from. Ports in overlay port groups and the overlay hipbr bridge interfaces are supported.



- Optional** – If using a local device as the Mirror Destination, you can enter a GRE or session ID to distinguish the traffic being sent from this Mirror Source by including this value in the GRE/ERSPAN header of packets sent to a local device sync.
- Recommended** – Set performance settings for suggestions on setting Snap length, Rate limit, and source-specific BPF filters that override the Mirror Destination BPF filters (Example (BPF filter of “ip proto not 47” to exclude mirrored traffic and avoid loops). See [Adjust performance for mirrored traffic](#) on page 394 for guidance, or for more information on BPF filters, see [BPF Settings for Port Mirroring](#) on page 396.

5. Select **Update Settings**.



Note: You can set up different configurations for a Mirror Source Airwall Gateway to send traffic to different Mirror Destinations.

Adjust performance for mirrored traffic

Because mirroring traffic can impact your network performance, it is best practice to set one or all of the following performance adjustments on the Mirror Destination and Source Airwall Gateways to mitigate the performance impact.

Here are the performance adjustments you can make:

Snap length

Specify that when mirroring traffic, a Mirror Source Airwall Gateway should only copy this many bytes of the original packet. You can use this setting to get “headers only” with a small value (~64 bytes), and/or avoid fragmentation with a larger value (~1000 bytes). Specifying a full Ethernet frame size of 1514 bytes will avoid truncating packets (if you are using 802.1q VLAN tags or jumbo frames you will need to increase this value), but results in fragmenting every full-size mirrored packet, doubling the number of packets which must be processed.

Rate limits

Set a rate limit for mirrored traffic. This limit is only applied to the mirrored copy of the traffic. It is a best practice to configure a rate limit to limit the performance impact of using mirroring so you don't negatively impact other traffic secured by the Airwall Gateway. This limit also protects against misconfigurations where the mirrored traffic itself is mirrored, resulting in infinitely mirroring the same packet.

As a starting point, here are some recommended values to not significantly impact existing traffic, based on the relative performance for specific Airwall Gateway models:

Airwall Gateway model	Suggested Rate Limit
100	1 Mb/s

110	3 Mb/s
75	5 Mb/s
150	10 Mb/s
250	15 Mb/s
300v	20-100Mb/s
500	100 Mb/s

 **Note:** You may want to set these limits lower, depending on your network bandwidth, particularly if your network connection is metered, as with a cellular provider.

When setting rate limits, also consider the performance of the Mirror Destination Airwall Gateway, the packet analyzer, and network connection between these Airwall Gateways.

BPF Filters

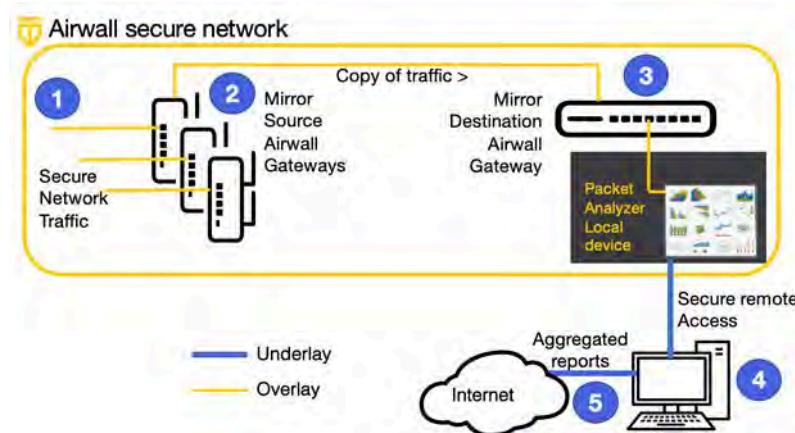
You can select which traffic is mirrored by specifying a BPF filter. If no filter is specified, all traffic is mirrored. By default, Mirror Source Airwall Gateways use the BPF filters specified on the Mirror Destination Airwall Gateway. You can override this default by setting different filters on any of the Mirror Source Airwall Gateways. BPF filters will filter mirrored traffic to specific protocols using BPF filter expressions. For information on the BPF filters most helpful for port mirroring, see [BPF Settings for Port Mirroring](#) on page 396.

Set up security for mirrored traffic

Protect your mirrored traffic.

Because your packet analyzer can be a back door to sensitive information about your network (impacting your Airwall secure network invisibility), you need to set up security policies to limit access to your packet analyzer and mirrored traffic so that only trusted devices can access it.

 **CAUTION:** It is a best practice to keep all of the information being sent to your packet analyzer within the Airwall secure network. Since you are essentially making a copy of potentially-sensitive overlay traffic and decrypting it for the packet analyzer, there is a risk of exposure if your packet analyzer is compromised, not secured, or if the network information you are capturing is sent over an unsecured network. You can secure the packet analyzer management interface within the Airwall secure network, with access to the interface limited to authorized personnel.



Configure your packet analyzer tool

Make sure your packet analyzer tool is set up to receive the mirrored network traffic data.

You should now be getting traffic to your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information) and can configure your packet analyzer software to consume the data being received from the Mirror Destination Airwall Gateway. For assistance, see the documentation for your packet analyzer software.

Verify Port Mirroring

To verify that port mirroring is working, check that data is flowing to your packet analyzer.

You can also:

- Check the Diagnostics reports on the Mirror Source and Destination Airwall Gateways and look for `aircap` processes. Aircap is the process that implements port mirroring.
- Check that there is a tunnel established from the Mirror Source Airwall Gateways to the Mirror Destination Airwall Gateway.
- You can check that there is traffic flowing from the Mirror Destination Airwall Gateway to the packet analyzer local device or Mirror Destination group.

BPF Settings for Port Mirroring

Specifying BPF filters for port mirroring will filter the traffic that is mirrored to your Mirror Destination Airwall Gateway. If you do not specify any filters, it will mirror all traffic.

Here are some sample BPF filters:

Filter Mirrored Traffic to Include/ Exclude	BPF Filter Format	Description and Examples
Traffic using a specific IP protocol	<code>ip proto <protocol_to_include></code> <code>ip proto not <protocol_to_exclude></code>	Mirror only traffic using IP protocol of IPv6. Examples: Only include IPv6 traffic: <code>ip proto 41</code>
All traffic on the specified host	<code>host <host_ip></code>	Don't include IPv4 traffic: <code>ip proto not 4</code>
All traffic where the specified host is the source	<code>src host <host_ip></code>	<code>host 192.0.2.10</code>
Exclude IP traffic	<code>no ip</code>	<code>src host 192.0.2.10</code>
All traffic on the specified port	<code>port <port_#></code>	<code>no ip</code>
All traffic on the ports in the specified range	<code>portrange <port1_#>-<port2_#></code>	<code>port 443</code>
		<code>portrange port 443-450</code>

Filter Mirrored Traffic to Include/ Exclude	BPF Filter Format Description and Examples																																																																																																																																																																																																									
Specific data	<p>You can combine conditions to narrowly match specific protocols like:</p> <pre data-bbox="1067 375 1372 435">udp port 10500 and udp[8:4] == 0</pre> <p>This filter matches UDP traffic with a source or destination port of 10500 and the first 32 bits of the UDP payload is zero. This matches HIP (control) protocol traffic excluding tunneled overlay traffic.</p>																																																																																																																																																																																																									
Specific devices and protocols	<table border="1" data-bbox="784 671 1632 783"> <thead> <tr> <th>Octet</th> <th>Bit</th> <th>0</th> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> <th>6</th> <th>7</th> <th>8</th> <th>9</th> <th>10</th> <th>11</th> <th>12</th> <th>13</th> <th>14</th> <th>15</th> <th>16</th> <th>17</th> <th>18</th> <th>19</th> <th>20</th> <th>21</th> <th>22</th> <th>23</th> <th>24</th> <th>25</th> <th>26</th> <th>27</th> <th>28</th> <th>29</th> <th>30</th> <th>31</th> <th>32</th> <th>33</th> <th>34</th> <th>35</th> <th>36</th> <th>37</th> <th>38</th> <th>39</th> <th>40</th> <th>41</th> <th>42</th> <th>43</th> <th>44</th> <th>45</th> <th>46</th> <th>47</th> <th>48</th> <th>49</th> <th>50</th> <th>51</th> <th>52</th> <th>53</th> <th>54</th> <th>55</th> <th>56</th> <th>57</th> <th>58</th> <th>59</th> <th>60</th> <th>61</th> <th>62</th> <th>63</th> <th>64</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td colspan="16">Source Port</td> <td colspan="16">Destination Port</td> </tr> <tr> <td>4</td> <td>32</td> <td colspan="16">Length</td> <td colspan="16">Checksum</td> </tr> <tr> <td>8</td> <td>64</td> <td colspan="64">ESP SPI == 0 (indicates HIP protocol traffic)</td> </tr> </tbody> </table> <p>Match HTTP packets where the payload starts with GET:</p> <pre data-bbox="1067 903 1323 984">tcp port 80 and tcp[20:4] == 1195725856</pre> <p>1195725856 is GET represented as a 32-bit network byte order integer.</p> <p>Mirror traffic for devices on specific hosts and ports:</p> <pre data-bbox="1067 1205 1437 1286">ip host 192.0.2.10 and (tcp port 80 or tcp port 443)</pre> <pre data-bbox="1067 1343 1437 1402">ip host 192.0.2.11 and udp port 53</pre>	Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	0	0	Source Port																Destination Port																4	32	Length																Checksum																8	64	ESP SPI == 0 (indicates HIP protocol traffic)																																																															
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64																																																																																																																																								
0	0	Source Port																Destination Port																																																																																																																																																																																								
4	32	Length																Checksum																																																																																																																																																																																								
8	64	ESP SPI == 0 (indicates HIP protocol traffic)																																																																																																																																																																																																								

Filter Mirrored Traffic to Include/ Exclude	BPF Filter Format	Description and Examples
Exclude high bandwidth service or known traffic	not (ip net <high_bandwidth_IP address> and tcp port <port_number>)	Exclude all HTTPS traffic to/from 192.0.2.0/24:  <pre>not (ip net 192.0.2.0/24 and tcp port 443)</pre> <p>Note: This filter can also work well with rate limiting. By excluding the known traffic (legitimate), you can mirror all of the other traffic and capture a greater portion of the anomalies with a small throughput and processing overhead.</p>

Port Mirroring BPF Reference

To create your own variations, here are the most useful BPF filter choices:

What to Filter

- IP host / network
- IPv6 host / network
- TCP / UDP port

Logical Operators

- and
- or
- not

 **Note:** Identifiers that are also a keyword must be escaped using a backslash (\). For example: ip proto \icmp. You can also refer to protocols by number. See <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml> as a reference. In this case, the above would be ip proto 1.

For more information on BPF filters, refer to one of the BPF references available online, such as <https://biot.com/capstats/bpf.html>.

Mirrored Traffic Definitions

Port Mirroring

Making a copy of some/all traffic crossing a specific physical port (for example, a network interface) and delivering this copy elsewhere. Usually used in conjunction with a packet analyzer.

SPAN

‘Switch Port Analyzer’ Cisco term for port mirroring.

TAP

An old way to mirror traffic – literally tap into network cable and connect to another network interface to receive a copy (wiretap).

Aircap	Airwall Solution's internal process used to implement port mirroring.
Packet analysis / packet dissection	Parsing packets to extract analytics.
Packet brokers	Industry term for packet analysis tools and related tools to transport mirrored packet to analysis tools.
GRE	'Generic Routing Encapsulation' an IP protocol used for encapsulation.
Mirror Destination	The Airwall Gateway mirrored traffic is sent to, either to a dedicated Mirror Destination group or to a packet analyzer connected as a local device to the overlay side of the Mirror Destination Airwall Gateway.
Mirror Sources	Airwall Gateways mirroring traffic and sending it to the Mirror Destination Airwall Gateway.

More Mirrored Traffic Scenarios

Typical scenarios for securely mirroring traffic to a packet analyzer and how to configure them.

There are many ways you can set up mirrored traffic. These scenarios give you an idea of how you can configure it so you are mirroring the traffic you want, and that mirrored traffic stays encrypted until it reaches its destination.

Mirroring Traffic on Airwall Gateways

- [Mirror Traffic to a Local Device destination \(Recommended Way\)](#)
- [Mirror traffic to a dedicated port](#) on page 400

Mirroring network traffic not on Airwall Gateways

- [Mirror non-Airwall network traffic](#) on page 405

Configuration Options

You can set up your network to mirror traffic in many different ways. Most combinations of Mirror Destination and Sources are valid. Whichever way you choose, you'll also need to do the following to ensure the security of mirrored traffic and make sure your port mirroring configuration is not negatively impacting performance on your network:

- [Adjust performance for mirrored traffic](#) on page 394
- [Set up security for mirrored traffic](#) on page 395
- [Configure your packet analyzer tool](#) on page 395
- [Verify Port Mirroring](#) on page 396

Options to connect your packet analyzer tool

You can connect your packet analyzer tool to your mirror destination in two ways:

- [Create a local device for your packet analyzer tool](#) on page 391
- [Connect your packet analyzer tool to a dedicated port](#) on page 401

Mirror Destination Options

- [Configure a Mirror Destination to send to a Local Device](#) on page 392
- [Configure a Mirror Destination to send to a Mirror Destination Group](#) on page 401

Mirror Source Options

- Configure Airwall Gateways to act as the Mirror Sources on page 393
- Mirror non-Airwall traffic to an Overlay port group on page 407

More Port Mirroring Possibilities

These diagrams show more supported ways to mirror traffic and connect a packet analyzer tool: [Diagrams for Port Mirroring](#) on page 409

Mirror traffic to a dedicated port

You can send mirrored traffic to a dedicated port group attached to a physical cable.

When using a dedicated port to connect the Mirror Destination Airwall Gateway to your packet analyzer, normal switches don't work. Since port mirroring captures traffic both directions, MAC flows are both directions. The switch learns all the MACs are connected to the Mirror Destination group and suppresses all traffic but broadcast, multicast, and unknown unicast MAC destinations.



Note: This configuration is not supported on the Airwall Gateway 300v model, because hypervisor has a switch.

Mirror traffic to a dedicated port

To mirror traffic to a dedicated port, you need to:

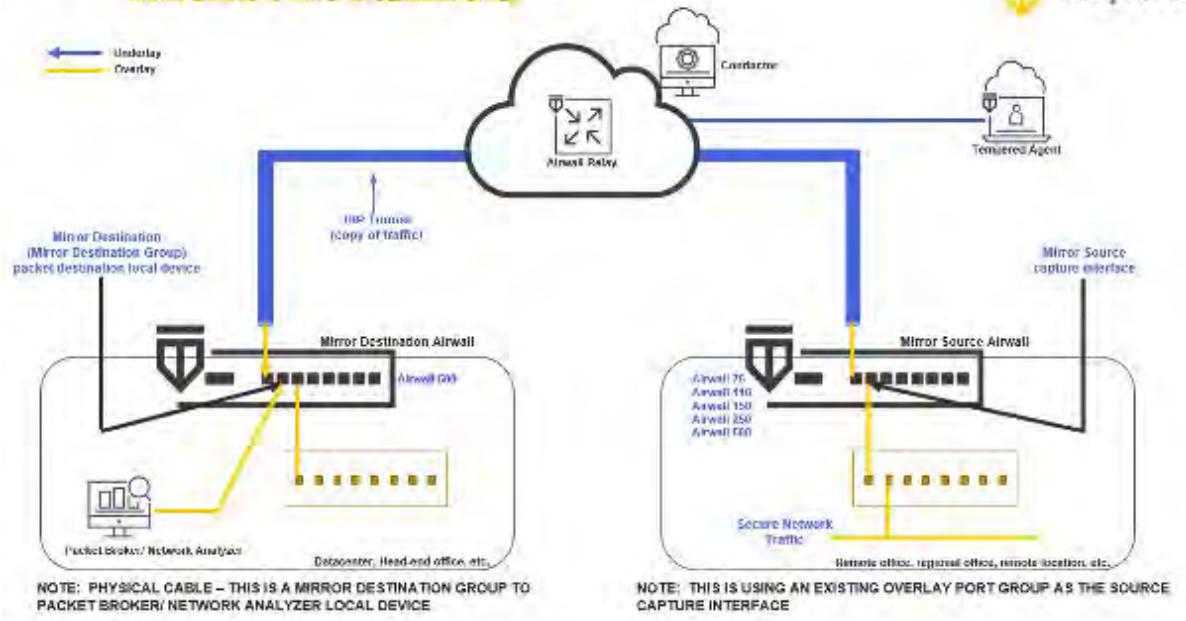
1. Connect your packet analyzer tool to a dedicated port on the Airwall Gateway you want to use as the Mirror Destination.
2. On the same Airwall Gateway, create a Mirror Destination port group, and assign the port your analyzer is plugged into to that group.
3. Configure a Mirror Destination to send to that Mirror Destination port group.
4. Configure Airwall Gateways to act as the Mirror Sources.
5. Adjust performance for mirrored traffic.
6. Set up security for mirrored traffic.
7. Configure your packet analyzer tool.

These steps are described in more detail in the following sections.

Here is a diagram showing this scenario:

Physical Airwall to Physical Airwall

Mirror Source to Mirror Destination Group



Connect your packet analyzer tool to a dedicated port

Directly connect your packet analyzer tool to a dedicated port on a physical Airwall Gateway.

1. Use a physical cable to connect your packet analyzer to a free port on the Airwall Gateway you'll be using as the Mirror Destination.
2. In Conductor, on this Airwall Gateway, go to **Ports > Port configuration**.
3. Select **Edit Settings**.
4. Next to **Port Groups**, select the + to add a port group.
5. Choose Mirror Destination group.
6. Expand the group, and give it a descriptive name.
7. Under **Interfaces**, select an unused port:

Ports	Assigned	IP address	MAC	Default gateway	MTU	VLAN
Port 1 Port 2 Port 3 Port 3	✓	192.168.1.51/24	00:0c:29:8e:1c	192.168.1.34	1500	

Port groups
Overlay Port Group 1
Overlay Port Group 1
Mirror Destination Port Group

Name	Interface
Mirror Destination Port Group	Port 3

8. Select **Update Settings**.

If you are using this method to connect your packet analyzer tool, you need to configure your mirror destination as described on this page: [Configure a Mirror Destination to send to a Mirror Destination Group](#) on page 401.

Configure a Mirror Destination to send to a Mirror Destination Group

The Mirror Destination Airwall Gateway is where the network information your packet analyzer needs to consume is sent.

When using a port group, you connect your packet analyzer to the Mirror Destination Airwall Gateway using a physical cable.

CAUTION: When you are using a Mirror Destination group as the destination, you can't use a normal or virtual switch – you must connect the Mirror Destination to the packet analyzer directly with a cable. Because of this, this configuration is not supported on the 300v.

1. On the Mirror Destination Airwall Gateway, go to **Ports > Port mirroring**.

2. Select **Edit Settings**.
3. Next to **Configurations**, select the + to add a port mirroring configuration.
4. In your new configuration:
 - a) Set the **Enabled** toggle to On.



Note: After configuration, use this toggle to turn port mirroring on and off.

- b) Under **Type**, select **Mirror Destination**.
- c) Under **Packet destination**, select the Mirror Destination group you set up earlier.
- d) **Optional** – Under **Overlay IP**, change the Airwall Gateway mirroring configuration IP address. This IP is used for internal addressing only and is set by default to fd00::/8.



CAUTION: When using Mirror Destination group, make sure it's not connected back to the original network, as this can cause loops with ever-increasing traffic as you're mirroring mirrored traffic (with the potential for overloading your network).

- e) **Optional** – Under **BPF filter**, Leave blank unless you are only interested in a single type of traffic, or want to exclude traffic from all sources.



Note: If you use a BPF expression on the Mirror Destination, that's the default for all of the Mirror Sources, unless you set a BPF expression on the source, which overrides this default.

5. Select **Update Settings**.

You should be able to see some traffic from the Mirror Destination Airwall Gateway to the Mirror Destination group.

Configure Airwall Gateways to act as the Mirror Sources

You configure Mirror Source Airwall Gateways to send network information to the Mirror Destination Airwall Gateway.



CAUTION: If you capture traffic on all ports of the overlay port group, you may set up a loop. To avoid this, in your configuration set a BPF filter of “ip proto not 47” to exclude mirrored traffic. See [BPF Settings for Port Mirroring](#) on page 396.

If you use GRE Transparent Ethernet Bridging, ERSPAN type II or ERSPAN type III – You can use GRE key or Session ID to identify which source the packets arrived on.

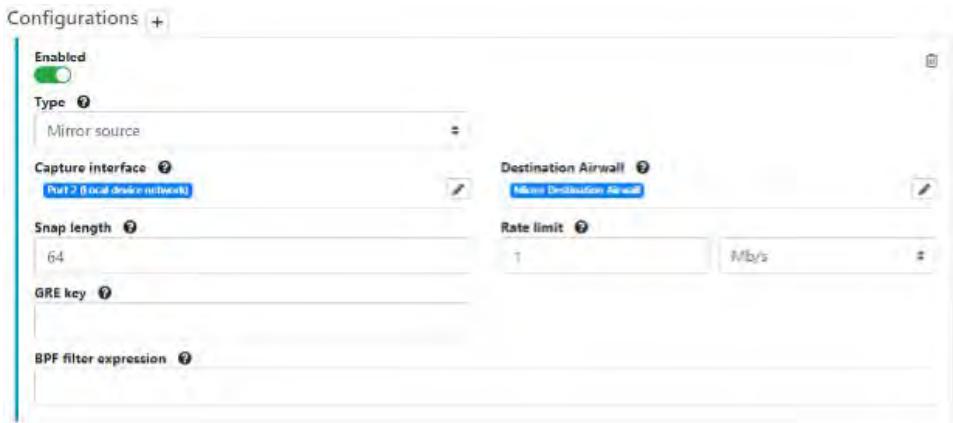


Note: You can set up the Mirror Destination to also be a Mirror Source, to include that Airwall Gateway's traffic in the information sent to the packet analyzer. In this case, be sure to set a BPF filter to exclude the mirrored traffic.

1. On a Mirror Source Airwall Gateway, go to **Ports > Port mirroring**.
2. Select **Edit Settings**.
3. Next to **Configurations**, select the + to add a mirroring configuration.

4. In your new configuration:

- Under **Type**, select Mirror Source.
- Under **Destination Airwall**, select the Airwall Gateway you set up as the Mirror Destination.
- Under **Capture interface**, select the interface you want to capture network information from. Ports in overlay port groups and the overlay hipbr bridge interfaces are supported.



- Optional** – If using a local device as the Mirror Destination, you can enter a GRE or session ID to distinguish the traffic being sent from this Mirror Source by including this value in the GRE/ERSPAN header of packets sent to a local device sync.
- Recommended** – Set performance settings for suggestions on setting Snap length, Rate limit, and source-specific BPF filters that override the Mirror Destination BPF filters (Example (BPF filter of “ip proto not 47” to exclude mirrored traffic and avoid loops). See [Adjust performance for mirrored traffic](#) on page 394 for guidance, or for more information on BPF filters, see [BPF Settings for Port Mirroring](#) on page 396.

5. Select **Update Settings**.



Note: You can set up different configurations for a Mirror Source Airwall Gateway to send traffic to different Mirror Destinations.

Adjust performance for mirrored traffic

Because mirroring traffic can impact your network performance, it is best practice to set one or all of the following performance adjustments on the Mirror Destination and Source Airwall Gateways to mitigate the performance impact.

Here are the performance adjustments you can make:

Snap length

Specify that when mirroring traffic, a Mirror Source Airwall Gateway should only copy this many bytes of the original packet. You can use this setting to get “headers only” with a small value (~64 bytes), and/or avoid fragmentation with a larger value (~1000 bytes). Specifying a full Ethernet frame size of 1514 bytes will avoid truncating packets (if you are using 802.1q VLAN tags or jumbo frames you will need to increase this value), but results in fragmenting every full-size mirrored packet, doubling the number of packets which must be processed.

Rate limits

Set a rate limit for mirrored traffic. This limit is only applied to the mirrored copy of the traffic. It is a best practice to configure a rate limit to limit the performance impact of using mirroring so you don't negatively impact other traffic secured by the Airwall Gateway. This limit also protects against misconfigurations where the mirrored traffic itself is mirrored, resulting in infinitely mirroring the same packet.

As a starting point, here are some recommended values to not significantly impact existing traffic, based on the relative performance for specific Airwall Gateway models:

Airwall Gateway model	Suggested Rate Limit
100	1 Mb/s

110	3 Mb/s
75	5 Mb/s
150	10 Mb/s
250	15 Mb/s
300v	20-100Mb/s
500	100 Mb/s



Note: You may want to set these limits lower, depending on your network bandwidth, particularly if your network connection is metered, as with a cellular provider.

When setting rate limits, also consider the performance of the Mirror Destination Airwall Gateway, the packet analyzer, and network connection between these Airwall Gateways.

BPF Filters

You can select which traffic is mirrored by specifying a BPF filter. If no filter is specified, all traffic is mirrored. By default, Mirror Source Airwall Gateways use the BPF filters specified on the Mirror Destination Airwall Gateway. You can override this default by setting different filters on any of the Mirror Source Airwall Gateways. BPF filters will filter mirrored traffic to specific protocols using BPF filter expressions. For information on the BPF filters most helpful for port mirroring, see [BPF Settings for Port Mirroring](#) on page 396.

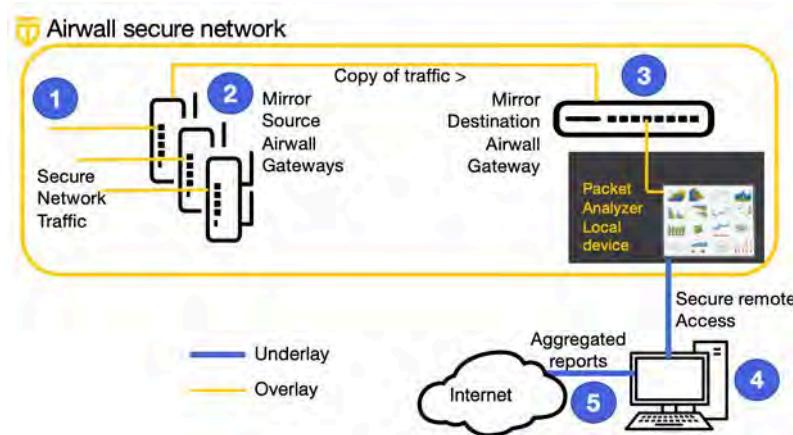
Set up security for mirrored traffic

Protect your mirrored traffic.

Because your packet analyzer can be a back door to sensitive information about your network (impacting your Airwall secure network invisibility), you need to set up security policies to limit access to your packet analyzer and mirrored traffic so that only trusted devices can access it.



CAUTION: It is a best practice to keep all of the information being sent to your packet analyzer within the Airwall secure network. Since you are essentially making a copy of potentially-sensitive overlay traffic and decrypting it for the packet analyzer, there is a risk of exposure if your packet analyzer is compromised, not secured, or if the network information you are capturing is sent over an unsecured network. You can secure the packet analyzer management interface within the Airwall secure network, with access to the interface limited to authorized personnel.



Configure your packet analyzer tool

Make sure your packet analyzer tool is set up to receive the mirrored network traffic data.

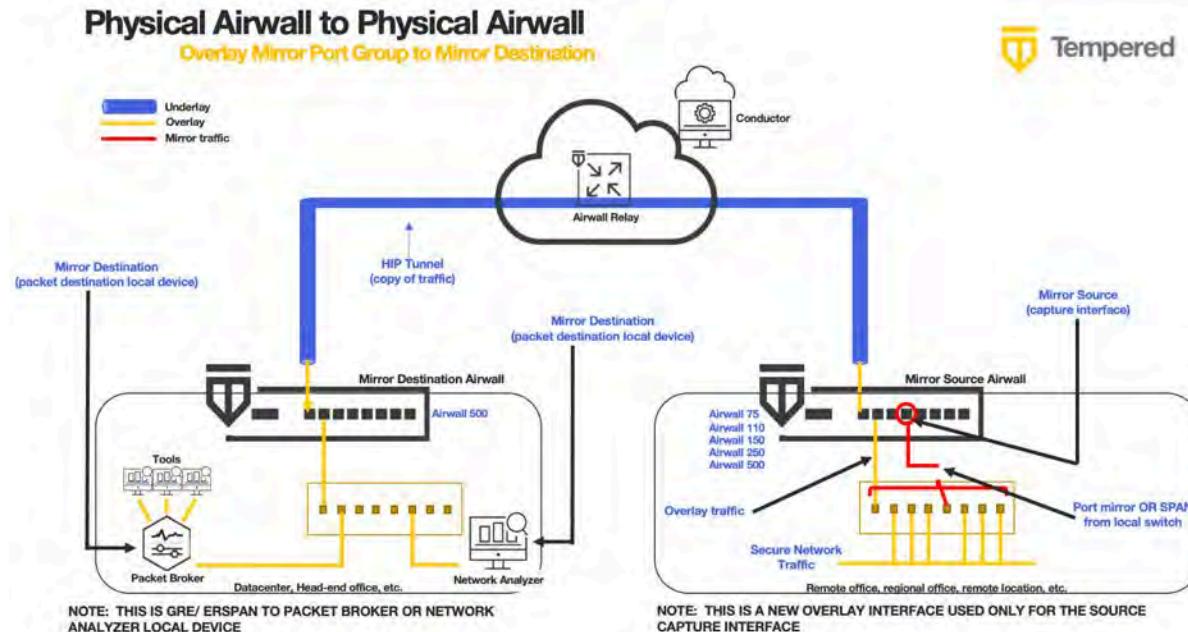
You should now be getting traffic to your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information) and can configure your packet analyzer software to consume the data being received from the Mirror Destination Airwall Gateway. For assistance, see the documentation for your packet analyzer software.

Mirror non-Airwall network traffic

Use this mirrored traffic scenario if you want to capture network traffic that isn't currently going through an Airwall Gateway. This method uses:

- **Mirror Destination** – A local device
- **Mirror Source** – A dedicated port and overlay port group on an Airwall Gateway that collects non-Airwall network traffic and sends to the Mirror Destination

This diagram shows how the traffic is mirrored and accessed, with mirrored traffic sent to a Mirror Source Airwall Gateway, then to the Mirror Destination Airwall Gateway over encrypted HIP Tunnels on the Underlay.



Set up this Mirrored Traffic Scenario

To configure this scenario, you need to:

1. Create a local device for your packet analyzer tool.
2. Configure a Mirror Destination to a Local Device.
3. Mirror non-Airwall traffic to an Overlay port group.
 - a) Add an Overlay Port group to capture non-Airwall traffic.
 - b) Add a Port Mirroring Configuration.
4. Adjust Performance for Mirrored Traffic.
5. Configure your network to send traffic to the Overlay Port group.
6. Connect your packet analyzer.

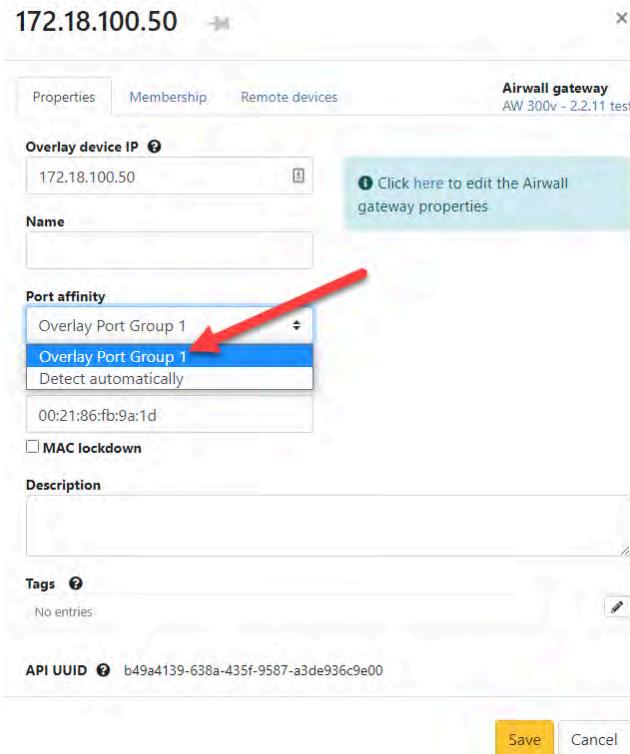
Create a local device for your packet analyzer tool

Create a local device on a dedicated overlay port group for your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information).

The destination for your mirrored traffic can be your packet analyzer set up as a local device on your Mirror Destination Airwall Gateway.

1. Add the packet analyzer tool as a local device to the Airwall Gateway that you're going to use as your Mirror Destination (the one that receives the mirrored traffic and sends it to the destination, which is your analyzer).

- When you're adding the device (either manually or through auto-discovery), you must set Port affinity (it can't be left on auto).



For more information, see [Add devices to the Conductor](#) on page 351.

If you are using this method to connect your packet analyzer tool, you need to configure your mirror destination as described on this page: [Configure a Mirror Destination to send to a Local Device](#) on page 392

Configure a Mirror Destination to send to a Local Device

The Mirror Destination Airwall Gateway receives the mirrored traffic and sends it to your packet analyzer (or network analyzer or packet broker).

If your packet analyzer supports receiving packets encapsulated in GRE or ERSPAN, this is the preferred configuration. It avoids the possibility of mirrored traffic being recirculated on your network and the MAC address table issues with switches. It also provides additional fields to your packet analyzer that allow it to distinguish between traffic captured by multiple Airwall Gateways (using GRE key/ERSPAN session ID) and detect lost or reordered packets (using ERSPAN sequence number).

- On the Airwall Gateway page, go to **Ports > Port mirroring**.
- Select **Edit Settings**.
- Next to **Configurations**, select the + to add a mirroring configuration.

4. In your new configuration:

- a) Set the **Enabled** toggle to On.



Note: After configuration, use this toggle to turn mirroring on and off.

- b) Under **Type**, select **Mirror Destination**.

- c) Under **Packet destination**, select the local device for your packet analyzer you set up earlier.



Note: The device will not show up as destination when you're selecting the Mirror Destination Airwall Gateway unless you've set a specific port group affinity (not Auto). See [Create a local device for your packet analyzer tool](#) on page 391.

- d) Under **Encapsulation type**, select the encapsulation (GRE or ERSPAN Type I, II, or III) supported by your packet analyzer. For example, for Nozomi, pick ERSPAN type II. Refer to documentation of your packet analyzer to determine which encapsulations it supports.



- e) **Optional** – Enter any information allowed for the type you selected (for example, GRE key or session ID).

- f) **Optional** – Under BPF filter, add any BPF filters you would like to use to filter the traffic that is mirrored to this Mirror Destination. See [BPF Settings for Port Mirroring](#) on page 396.



Note: If you use a BPF expression on the Mirror Destination, that's the default for all of the Mirror Sources, unless you set a BPF expression on the source, which overrides this default.

5. Select **Update Settings**.

You should be able to see some traffic from the Mirror Destination to the packet analyzer local device.

Mirror non-Airwall traffic to an Overlay port group

To capture mirrored non-Airwall traffic, you can configure an Overlay Port Group on a Mirror Source Airwall Gateway, which then sends network information to the Mirror Destination Airwall Gateway.

For this scenario, you need to add an overlay port group to capture non-Airwall traffic and a Mirror Source port mirroring configuration that captures the mirrored traffic on that port.

If you use GRE Transparent Ethernet Bridging, ERSPAN type II or ERSPAN type III – You can use GRE key or Session ID to identify which source the packets arrived on.

1. Set up an Overlay port group on a Mirror Source Airwall Gateway to capture the non-Airwall traffic being collected by your network:



- Add a Port Mirroring Configuration on the same Airwall Gateway, selecting the port you configured as your Port Mirror (SPAN) Overlay group above as the Capture interface, and the Mirror Destination:

For details on how, see [Configure Airwall Gateways to act as the Mirror Sources](#) on page 393

Adjust performance for mirrored traffic

Because mirroring traffic can impact your network performance, it is best practice to set one or all of the following performance adjustments on the Mirror Destination and Source Airwall Gateways to mitigate the performance impact.

Here are the performance adjustments you can make:

Snap length

Specify that when mirroring traffic, a Mirror Source Airwall Gateway should only copy this many bytes of the original packet. You can use this setting to get “headers only” with a small value (~64 bytes), and/or avoid fragmentation with a larger value (~1000 bytes). Specifying a full Ethernet frame size of 1514 bytes will avoid truncating packets (if you are using 802.1q VLAN tags or jumbo frames you will need to increase this value), but results in fragmenting every full-size mirrored packet, doubling the number of packets which must be processed.

Rate limits

Set a rate limit for mirrored traffic. This limit is only applied to the mirrored copy of the traffic. It is a best practice to configure a rate limit to limit the performance impact of using mirroring so you don't negatively impact other traffic secured by the Airwall Gateway. This limit also protects against misconfigurations where the mirrored traffic itself is mirrored, resulting in infinitely mirroring the same packet.

As a starting point, here are some recommended values to not significantly impact existing traffic, based on the relative performance for specific Airwall Gateway models:

Airwall Gateway model	Suggested Rate Limit
100	1 Mb/s
110	3 Mb/s
75	5 Mb/s
150	10 Mb/s
250	15 Mb/s
300v	20-100Mb/s
500	100 Mb/s



Note: You may want to set these limits lower, depending on your network bandwidth, particularly if your network connection is metered, as with a cellular provider.

When setting rate limits, also consider the performance of the Mirror Destination Airwall Gateway, the packet analyzer, and network connection between these Airwall Gateways.

BPF Filters

You can select which traffic is mirrored by specifying a BPF filter. If no filter is specified, all traffic is mirrored. By default, Mirror Source Airwall Gateways use the BPF filters specified on the Mirror Destination Airwall Gateway. You can override this default by setting different filters on any of the Mirror Source Airwall Gateways. BPF filters will filter mirrored traffic to specific protocols using BPF filter expressions. For information on the BPF filters most helpful for port mirroring, see [BPF Settings for Port Mirroring](#) on page 396.

Configure your network to send traffic to the Overlay port group

Send your non-Airwall traffic to the Mirror source Airwall Gateway.

Connect your network to the port for the Overlay port group created on the Mirror Source Airwall Gateway, and follow the instructions for your network to gather and send traffic to that port.

Configure your packet analyzer tool

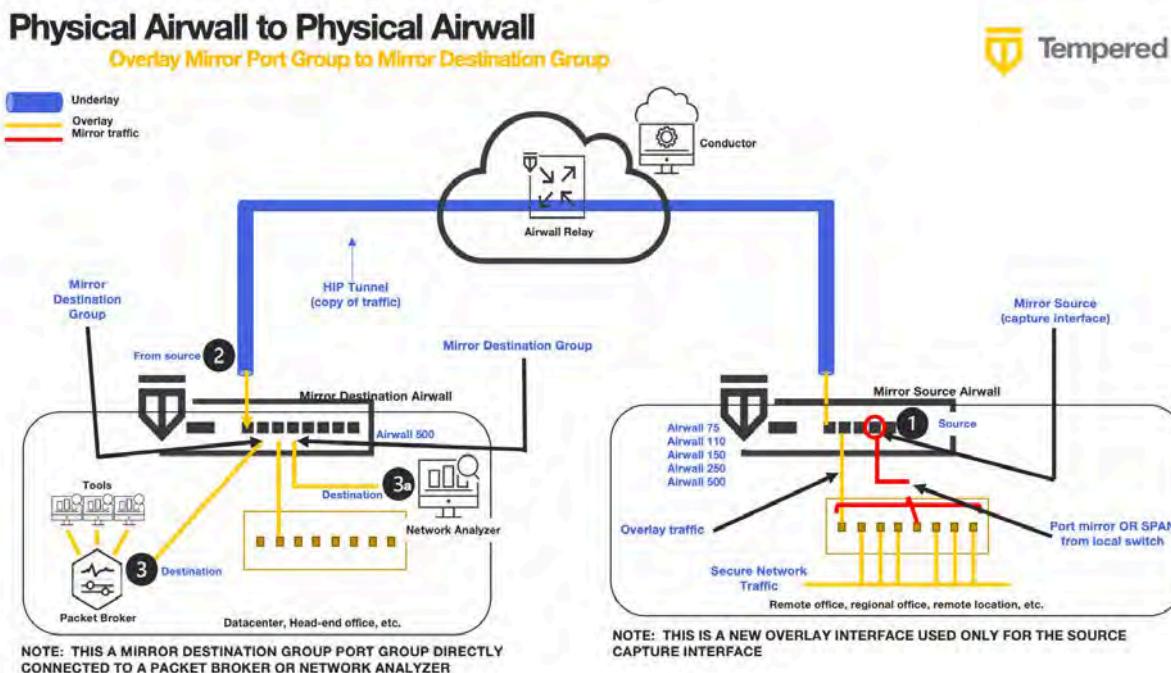
Make sure your packet analyzer tool is set up to receive the mirrored network traffic data.

You should now be getting traffic to your packet analyzer tool (protocol analyzer, packet broker, or other tool that consumes network traffic information) and can configure your packet analyzer software to consume the data being received from the Mirror Destination Airwall Gateway. For assistance, see the documentation for your packet analyzer software.

Diagrams for Port Mirroring

More supported configurations to mirror traffic.

Overlay Mirror Port Group to Mirror Destination Group

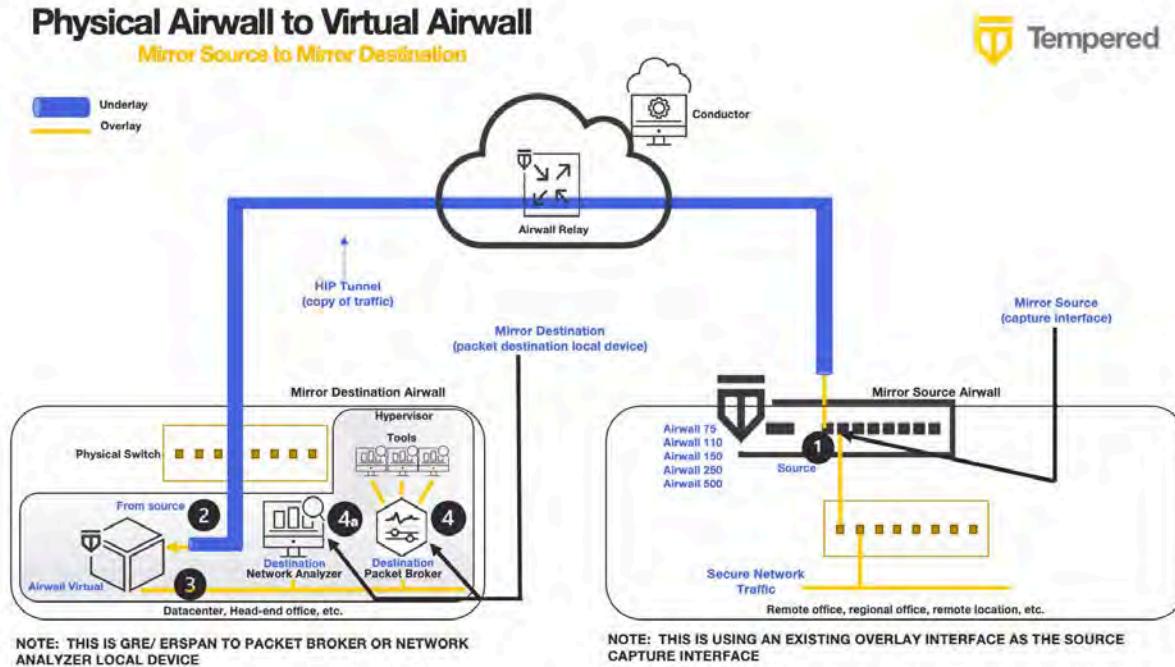


To set up this configuration:

1. Connect your packet analyzer tool to a dedicated port on page 401
2. Configure a Mirror Destination to send to a Mirror Destination Group on page 401
3. Mirror non-Airwall traffic to an Overlay port group on page 407
4. Adjust performance for mirrored traffic on page 394
5. Configure your network to send traffic to the Overlay port group on page 409

6. Configure your packet analyzer tool on page 395
7. Verify Port Mirroring on page 396

Physical Mirror Source to Virtual Mirror Destination



To set up this configuration:

1. Connect your packet analyzer tool to a dedicated port on page 401
2. Configure a Mirror Destination to send to a Mirror Destination Group on page 401
3. Configure Airwall Gateways to act as the Mirror Sources on page 393
4. Adjust performance for mirrored traffic on page 394
5. Set up security for mirrored traffic on page 395
6. Configure your packet analyzer tool on page 395
7. Verify Port Mirroring on page 396

Diagnostics and Troubleshooting

Diagnostic Tools

Put the Conductor into diagnostic mode

Placing the Conductor into diagnostic mode requires console access with a VGA monitor and USB keyboard.

When the Conductor is in diagnostic mode, you can:

- Download a Conductor support bundle. You can also download a support bundle from the Conductor if it's running. See [Create a support bundle from the Conductor](#) on page 412.
- Display system status. You can also see system status on the Conductor Dashboard. See [The Conductor Dashboard](#) on page 32.
- Perform firmware updates. You can also easily apply firmware updates in the Conductor. See [Update your Conductor and Airwall Edge Services](#) on page 106.
- Enable and disable SSH (SSH is disabled by default). See [Set up Remote Access to Airshell](#) on page 310.

To put the Conductor into diagnostic mode

1. Connect your laptop to port 2 of the Conductor's, and configure your laptop adapter to use DHCP.
2. At the login prompt:

- 2.2.3 and later: Enter `airsh` to enter the console, and then enter `diag`.



Note: If you're asked for a password, enter the default password `airsh`, or the password you set.

- Earlier than 2.2.3: Enter `diag` then enter the password `diag`.

3. Once your laptop obtains an IP address, open a web browser and navigate to `http://192.168.56.3` and the Conductor diagnostic page loads.

Once the Conductor is in diagnostic mode, Overlay network communications from the Conductor are disabled and device network is reconfigured with a static IP address.



Note: To exit diagnostic mode, select **Reboot** in the Diagnostic mode interface, or turn the Conductor off and back on again.

For more information on console commands, see [Airwall Gateway Airshell console commands – airsh](#) on page 305.

Put an Airwall Gateway into diagnostic mode

With an Airwall Gateway in diagnostic mode, you can troubleshoot it by collecting diagnostic information and you can also manage a variety of settings such as IP addresses, logs, and firmware.

After placing an Airwall Gateway in diagnostic mode, you must restart it to return it to normal operating mode. After restarting, the Airwall Gateway may require up to 3 minutes to return to operating mode.



Important: Do not continue pressing the Multi-Purpose or Reset button after 3 seconds as this will reset the Airwall Gateway to factory settings.

There are many Airwall Gateway diagnostic tasks you can do in the Conductor if it has access. See [Diagnostics and Troubleshooting](#) on page 410.



Note: See the platform guide that came with your Airwall Gateway for specific instructions for your model. If you are using versions before 2.2.3, please see the [2.2.3 help](#).

1. Airwall Gateway 100, 110, 150, 200, and 250 - Place into diagnostic mode by pressing and holding the Multi-Purpose or Reset button for only three seconds. Immediately release the button.
After three seconds, the status LED blinks to indicate the Airwall Gateway is in Diagnostic Mode. For more information about LED blink patterns, see your platform guide.
2. Airwall Gateway 300, 400, and 500 series - Place into diagnostic mode by connecting a VGA monitor and a USB keyboard to port 2 of the Airwall Gateway, and at the login prompt:
 - 2.2.3 and later: Enter `airsh` to enter the console, and then enter `diag`.



Note: If you're asked for a password, enter the default password `airsh`, or the password you set.

- Earlier than 2.2.3: Enter `diag` then enter the password `diag`.

3. Once your laptop obtains an IP address, open a web browser and navigate to `http://192.168.56.3` and the Conductor diagnostic page loads.

Once the Airwall Gateway is in diagnostic mode, Overlay network communications from the Airwall Gateway are disabled and device network is reconfigured with a static IP address.

1. Connect a computer to one of the device network ports. The computer will use DHCP to obtain an IP address from the Airwall Gateway.
2. Connect your web browser to `http://192.168.56.3` to access the Airwall Gateway diagnostic page.



Note: To exit diagnostic mode, select **Reboot** in the Diagnostic mode interface, or turn the Airwall Gateway off and back on again.

For more information on console commands, see [Airwall Gateway Airshell console commands – airsh](#) on page 305. See also [Connect an Airwall Gateway with Diag mode](#) on page 246.

Create a Conductor database backup

A Conductor database backup can provide a measure of security when you are working on system-wide changes. Before you update firmware or replace hardware, we strongly recommend that you create, download and archive a Conductor database backup.



CAUTION: Do not attempt to restore a Conductor from a database backup that was running a previous firmware revision.

To create a database backup:

1. Log in to Conductor as a system administrator
2. Go to **Settings** and open the **Diagnostics** tab.
3. Under **Diagnostics**, select **Download database backup**.
4. Click **Create**.
5. Once the backup is complete, select **Download the backup archive** and save the backup file.

Restore or replace a Conductor database backup



Note: The Conductor database can be restored using a backup file; however, all changes to the Conductor configuration made after database backup creation will be lost.

To restore a Conductor from a previously created database backup, go to **Settings**, and select **Restore a database backup**. Choose the database backup file and click **Upload**.



Important: A Conductor cannot be restored using a database backup taken while running a previous firmware version.

Upgrade or replace a Conductor

If you are upgrading or replacing your Conductor, we strongly recommend that you first create a database backup as described above and download to your desktop or similar. Once the Conductor database backup has been created and downloaded, do not make any configuration changes. When the replacement Conductor is online, navigate to 192.168.56.2 and login as the System Administrator. Go to **Settings**, select **Restore a database backup**, choose the database backup file and click **Upload**. Next, take the existing Conductor offline and set the network configuration of the replacement Conductor so it is identical to the network configuration of the existing Conductor. Your Airwall Edge Services will begin communicating with the new Conductor. You can verify status in the **Dashboard** of the Conductor.

Create a support bundle from the Conductor

To facilitate customer troubleshooting, Customer Success may request a Conductor support bundle

To create a Conductor support bundle

1. Go to **Settings**, click **Support Functions**, and select **Download a Conductor support bundle**. The Conductor creates a support bundle and provides it as a downloadable file.
2. Download the support bundle file and send to Customer Success support@tempered.io.

Customer Success can then analyze this encrypted support bundle.



Note: You can also download the most recent Conductor support bundle from the following URL:
https://<conductor-ip-address>/support/support_bundles/sc-support-bundle.

Troubleshoot an Airwall Gateway by creating a support bundle

Creating a support bundle is one of several diagnostic tools that you can use to help our support staff assist in troubleshooting an Airwall Gateway. The Conductor offers several diagnostic capabilities and you can learn about the others by using the links near the bottom of this article.

Support bundles are encrypted files. For security purposes, only Tempered can open them.

To create a support bundle:

1. Log in to the Conductor with a system administrator or network administrator role account.
2. Go to **Airwalls edge services**, open one from the list, and then open **Diagnostics**.



Note: If an Airwall Gateway is offline, you can put it into diagnostic mode and download a support bundle. See [Put an Airwall Gateway into diagnostic mode](#) on page 411 for more information.

3. Create your Airwall Gateway support bundle by clicking **Request a support bundle**.

Once the support bundle .pkg file has been created, you will be provided a download link to the file. A support bundle .pkg file is an encrypted archive that facilitates technical support by Tempered only.

4. Send the support bundle as an email attachment to support@tempered.io. A Tempered support engineer will contact you when it is received.

Troubleshoot an Airwall Gateway by creating a diagnostic report

Creating a diagnostic report is one of several diagnostic tools that you can use to get a general overview of the health of an Airwall Gateway. The Conductor offers several diagnostic capabilities and you can learn about the others by using the links near the bottom of this article.

To create a diagnostic report:

1. Go to **Airwalls edge services**, open one from the list, and then go to **Diagnostics**.

If an Airwall Gateway is offline, you can put it into diagnostic mode and download a support bundle. For more information, see [Put an Airwall Gateway into diagnostic mode](#) on page 411.

2. Create your report by clicking **Request a diagnostic report**.

Once the report .txt file has been created, you will be provided a download link to it. The diagnostic report is a text file that you can examine to see a high-level look at the overall health of the Airwall Gateway.

Update the MAC address (OUI) (Manufacturer) List

The OUI (organizationally unique identifier) list is used to map device MACs to manufacturer names in your **Devices** list. If the list has changed since you installed your Conductor, you can now update it.

1. Log in to Conductor as a system administrator.
2. Go to **Settings** and open the **Diagnostics** tab.
3. Under **Actions**, select **Update OUI list**.

You now see updated OUI information on Device pages, and in the **OUI** column of the **Devices** list. See [See MAC address OUI \(Manufacturer\) Information for Devices](#) on page 97.

Connection Troubleshooting

Help if you're having trouble connecting Airwall Edge Services to your Airwall secure network.

Airwall Agent, Server or Gateway using IPv6 has trouble connecting

If you have Airwall Agents or Airwall Gateways that are only getting a IPv6 address on cellular, and you want to connect to other Airwall Edge Services on IPv4, you need to have a relay policy set up on a dual stack (IPv4 + IPv6) Airwall Relay.

To do this, set both IPv4 and IPv6 IP addresses on the same underlay on the Airwall Relay, and enable bypass:



Capture network traffic on an Airwall Gateway

As part of the troubleshooting process, it is sometimes necessary to capture network traffic. The Airwall Gateway can capture traffic on the local interfaces as well as on the HIP tunnel from the Airwall Gateway to other Airwall Gateways.

All of these steps are done from a Conductor and require administrator permissions.

- Navigate to the Airwall Gateway you wish to capture from
- Select **Diagnostics**
- In Data capture, select **Start Packet Capture**
- Select the appropriate interface, if needed

Interface	Role	Usage
HIP tunnel	HIP Traffic	Use the HIP tunnel for protected traffic.
Internal	Internal Traffic	This captures the traffic that occurs within the local network.
Port 0	Underlay	This is the Port 2 (underlay) for traffic to/from the local network of the Airwall Gateway.
Port 1	Overlay	Use the Port 1 (overlay), for traffic to/from the protected device.

- Set any other options needed for the capture
- Click **Ok** to start the capture



CAUTION: The maximum file size is one quarter (1/4) of the available free space, so it is recommended that you set limits on the capture. In some models, such as the Airwall Gateway/HIPswitch 100, this can take up enough space to cause issues with upgrades.

Airwall Gateway link monitoring

Airwall Gateways have a utility to monitor its underlay network interfaces and determine if one is available for us.

Internet Control Message Protocol (ICMP) is a prerequisite for link monitoring to validate a link.

By default, an Airwall Gateway will prefer wired underlay interfaces to cellular or Wi-Fi.

2.0.x and earlier

Airwall Gateways running firmware versions prior to 2.1.0 have a limited functionality link monitoring utility. If a wired underlay interface has an IP address and can successfully ping its targets, it will use that interface.

The default monitor targets for Airwall Gateways running firmware before 2.1.0 are:

- Conductor
- Default Gateway
- DNS Servers

- Underlay IP addresses of all Airwall Gateway peers

If all of these targets fail, the Airwall Gateway will switch to its secondary network interface (cellular or Wi-Fi).

2.1.x and later

Starting in v2.1.x, the Airwall Gateway now implements a smart, configurable link monitor.

This new and improved link monitoring functions is fully configurable, allowing the following tunable options:

- Custom ping destinations (Conductor enabled by default)
- Ping rate (frequency), timeout, time to live (TTL), and failure count
- Disabling ping monitors on active link

Troubleshoot an Airwall Gateway by using packet capture

Packet capture is one of several diagnostic tools that you can use to facilitate troubleshooting an Airwall Gateway. The Conductor offers several diagnostic capabilities and you can learn about the others by using the links near the bottom of this article.

1. Go to **Airwalls edge services**, open one from the list, and go to **Diagnostics**.
2. Begin packet capture by clicking **Start Packet Capture** and then stop packet capture by clicking **Stop Packet Capture**.

Once the packet capture .pcap file has been created, you will be provided a download link to the file. The .pcap file is a standard format file that can be viewed with an application such as **Wireshark**.

Troubleshoot Initial Airwall Gateway connections

Here are some things to check if you are having trouble connecting your Airwall Gateway to your Conductor or underlay network.

- Check that the information you've entered for your WiFi or cellular service are correct.
- If you have a wired connection, check that it is connected to correct port for your Airwall Gateway. See your platform guide for instructions.
- Try pinging:
 - Ping the Conductor in Airshell:

```
airsh>> ping Conductor_IP_address
```
 - Ping a well-known service (such as Google DNS 8.8.8.8) to check for Internet connectivity:

```
airsh>> ping 8.8.8.8
```
 - Ping the default gateway for your network.

If pinging fails, get a packet capture from the Airwall Gateway and see where the ping is failing. For more information, see [Troubleshoot an Airwall Gateway by using packet capture](#) on page 415.

- Check that the interface has IP. You can get the IP address using the Airshell status command:

```
airsh>> status network  
airsh>> status cell  
airsh>> status wifi
```
- Check that the default route and link are up.
- Check that the following ports are open in your network firewall:
 - UDP 10500 - Check that both inbound and outbound connections are allowed.
 - TCP 8096 - Check that inbound connections are allowed.

To verify that TCP 8096 is working through any firewall connections:

```
netcat: nc -vz <Conductor-IP> port 8096
```

Bypass warning when connecting to the Conductor

Many browsers see the self-signed certificate on a new Conductor as a security risk. Here's how to proceed past the warning to the Conductor on several browsers. Sometimes after provisioning the Conductor, you will be able to bypass this warning. To prevent this error, [Install a Custom CA Certificate Chain](#) on page 201.

Google Chrome "Your connect is not private"

You may need to type `thisisunsafe` in the browser window to proceed past the warning. After you provision the Conductor, you will be able to bypass this warning by selecting Advanced and bypass.

Firefox

Select Advanced and then proceed to bypass.

Handle IP Conflicts

Learn how to identify and manage IP conflicts in your Airwall secure network.

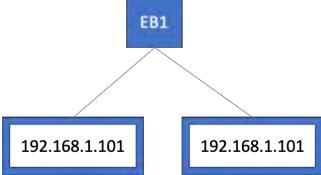
Your Airwall secure network can manage devices with the same IP as long as these duplicate IPs:

- Are not on the same Airwall Gateway, AND
- Do not have direct, indirect, or implicit policy between them in an overlay.

You can have duplicate IPs on the same overlay, as long as there is no policy between them.

If you are making a change that causes an IP conflict, the Conductor gives you an error message with information on the conflict.

The following diagrams show examples of IP conflicts, with suggestions for removing the conflict besides changing one of the IPs. If you want to have policy between the two, you have to change one of the IP addresses:

Conflict	No Conflict
Duplicate IPs on an Airwall Gateway  <pre> graph TD EB1[EB1] --- D1[192.168.1.101] EB1 --- D2[192.168.1.101] </pre>	Duplicate IPs on different Airwall Gateways, in the same overlay, but with no policy between them.  <pre> graph LR EB1[EB1] --- D1[192.168.1.101] EB2[EB2] --- D2[192.168.1.101] </pre>
Duplicate IPs (in the same or different overlays) with policy to each other  <pre> graph LR EB1[EB1] --- D1[192.168.1.101] EB2[EB2] --- D2[192.168.1.101] D1 -.-> D2 </pre>	Give devices with the same IP a NAT overlay device IP. See Resolve IP conflicts by giving duplicate devices a NAT IP address on page 417.

Conflict	No Conflict
Duplicate IPs in an overlay with policy to a shared IP <pre> graph TD EB1[EB1] --> 192_168_1_101[192.168.1.101] EB1 --> 192_168_1_103_1[192.168.1.103] EB1 --> 192_168_1_103_2[192.168.1.103] 192_168_1_103_1 --> EB2[EB2] 192_168_1_103_2 --> EB3[EB3] </pre>	Duplicate IPs in an overlay with policy to IPs on different Airwall Gateways, or give one of the devices a NAT overlay device IP. See Resolve IP conflicts by giving duplicate devices a NAT IP address on page 417.
Indirect conflict – Duplicate IPs in an overlay with policy to IPs on a shared Airwall Gateway. <pre> graph TD EB1[EB1] --> 192_168_1_101[192.168.1.101] EB1 --> 192_168_1_102[192.168.1.102] 192_168_1_101 --> 192_168_1_103_1[192.168.1.103] 192_168_1_102 --> 192_168_1_103_2[192.168.1.103] 192_168_1_103_1 --> EB2[EB2] 192_168_1_103_2 --> EB3[EB3] </pre>	Give devices with the same IP a NAT overlay device IP. See Resolve IP conflicts by giving duplicate devices a NAT IP address on page 417
Implicit conflict – IP in an overlay with policy to an IP that shares an Airwall Gateway with the same IP. <pre> graph TD EB1[EB1] --> 192_168_1_101[192.168.1.101] EB1 --> 192_168_1_102[192.168.1.102] 192_168_1_101 --> 192_168_1_102_1[192.168.1.102] 192_168_1_102_1 --> EB2[EB2] </pre>	Give devices with the same IP a NAT overlay device IP. See Resolve IP conflicts by giving duplicate devices a NAT IP address on page 417

Resolve IP conflicts by giving duplicate devices a NAT IP address

If you have an IP conflict, and want to have policy (set trust) between the conflicting IPs, you can often resolve the issue by giving any devices with duplicate IP addresses a NAT IP address.

It is important to understand the difference between the two IPs: overlay device IP and overlay device IP (NAT). The overlay device IP is both the local and overlay IP unless NAT is turned on. If NAT is on, then the overlay device IP

is only the local IP and the NAT IP is the overlay IP. Other Airwall Gateways only see the overlay IP, so the local IP cannot cause a conflict on them.

It is possible to change the local IP, but you have to be able to change it on the device itself. It is often easier to just NAT the IP if your conflict falls into one of the categories where NAT will fix it (see [Handle IP Conflicts](#) on page 416). Changing the device's actual IP and updating its overlay device IP should be reserved for situations that cannot otherwise be solved.

To give a device a NAT IP:

1. On the device's host Airwall Gateway, open the **Local devices** tab, **Configuration** subtab, and select **Edit Settings**.
2. On the right, under **Local device network configuration**, check **Enable NAT**.
3. In the **Local devices** table, enter a unique **Overlay device IP (NAT)** address for any devices that will conflict with another device that you want to create policy to (direct, indirect, or implicit – see [Handle IP Conflicts](#) on page 416).

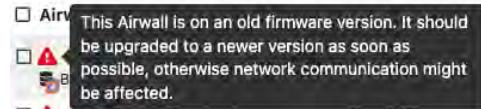
The screenshot shows the Airwall Gateway configuration interface. At the top, there are tabs for 'Airwall gateway', 'Local devices' (which is selected), and other network-related tabs. Below the tabs is a sub-tab for 'Configuration'. The main area is titled 'Local devices' and contains a table with three columns: 'Device name', 'Overlay device IP (NAT)', and 'Overlay device IP'. There are four rows in the table, each with a red exclamation mark icon next to the 'Overlay device IP (NAT)' field, indicating a conflict. To the right of the table is a sidebar with sections for 'Device discovery' (with a checked checkbox for 'Enable device discovery') and 'Local device network configuration' (with a checked checkbox for 'Enable NAT' followed by a red exclamation mark icon).

4. Select **Update Settings**.

Update v2.1.x Airwall Edge Services for the v3.0 Conductor

With this release, any Airwall Edge Services running v2.1.x releases will show an error recommending you update them. After updating Conductor to v3.0 or later, you won't be able to configure v2.1.x devices from the Conductor until you update them.

The red exclamation point next to the Airwall Edge Service indicates one that needs to be updated.



Updatev2.1.x Airwall Edge Services

1. Update any Airwall Edge Services running v2.1.x firmware to a v2.2.x firmware version first.
2. If desired, then update to v3.0 or later.

Configure v2.1.x Airwall Edge Services in a v3.0 or later Conductor

To configure v2.1.x Airwall Edge Services after updating the Conductor to v3.0 or later, you must update those services to v2.2.x or later as described above.

Factory Reset a Conductor

Reset aConductor to return it to the original factory settings. If an Airwall Edge Service is not online at the time of a factory reset, and an SRV record is configured for the MAP server in DNS, the Conductor performs these actions when the Airwall Edge Service next comes online.



Note: Factory resetting a Conductor requires console access with a VGA monitor and USB keyboard.

To reset the Conductor:

1. In the console at the login prompt, enter the username <factoryreset>.
2. At the password prompt, enter the password <factoryreset>.

Conductor will be factory reset.

Once a Conductor is factory reset, all Airwall Edge Services must be factory reset to re-connect to the Conductor, unless the Conductor configuration is restored from a Conductor database backup. To avoid this, download a Conductor database backup prior to doing a factory reset.

Factory Reset a Virtual Conductor

You can reset a virtual Conductor to return it to the original settings.

Once a Conductor is factory reset, all Airwall Edge Services must be factory reset to reconnect to the Conductor, unless the Conductor configuration is restored from a Conductor database backup. To avoid this, download a Conductor database backup prior to factory resetting a Conductor.

1. Display the console for the Conductor instance you would like to reset.
2. Enter `factoryreset` for user name and `factoryreset` for the password.

The Conductor will now revert to its factory default settings.

Reboot an Airwall Gateway

Rebooting an Airwall Gateway is one of several diagnostic techniques that you can use to help troubleshoot. For instructions on rebooting your Airwall Gateway, refer to its Product Guide.

Factory Reset an Airwall Gateway

You can reset Airwall Gateways to return them to the original factory settings. If an Airwall Gateway is not online at the time of a factory reset, and an SRV record is configured for the MAP server in DNS, the Conductor performs these actions when the Airwall Gateway next comes online.

To factory reset your Airwall Gateway, use the 'factoryreset' command. This command reverts the Airwall Gateway to factory settings, erasing all configuration settings, so use it with caution.

```
login: factoryreset
password: factoryreset
```

Once an Airwall Gateway is in the factory-reset state, it is placed into the unmanaged mode and one of the following scenarios will occur:

- The Airwall Gateway page in the Conductor shows a status as offline. Once the Airwall Gateway is factory reset, all devices attached to the Airwall Gateway are removed along with any additional user-provided information, such as name, location, overlay network and wireless configurations. To re-deploy a factory-reset Airwall Gateway, you must reconfigure the Airwall Gateway to point to the Conductor. Once configured, the Airwall Gateway appears in the Conductor with "factory reset" appended to its name.
- If you've [configured a DNS SRV record](#) for your Conductor, the Airwall Gateway automatically re-connects. After the Airwall Gateway connects, the Conductor removes it from any existing overlay networks, and appends (factory reset) to its name. The Conductor also removes all devices attached to the Airwall Gateway, as well as any additional user-provided information, such as human-friendly name or location. Cached overlay network and wireless configurations are also removed.

Revoke and Reactivate an Airwall Edge Service

If an Airwall Gateway, Airwall Agent, or Airwall Server is lost, stolen or damaged, you can revoke it to remove its access to your Airwall secure network. You must be a manager of all overlay networks to which the Airwall Edge

Service belongs. Once revoked, the Airwall Edge Service will not be able to establish or receive communications on your Airwall secure network.

To revoke an Airwall Edge Service:

1. Log in as an administrator with manager access rights to the overlays the Airwall Edge Service belongs to.
2. Go to the **Airwalls** page, and find the Airwall Edge Service you want to revoke.
3. Open the actions menu with the arrow to the right of the Airwall Edge Service, and select **Revoke**.
4. In the confirmation dialog, click **Apply**.

The Airwall Edge Service is revoked and "revoked" is added to its name. By default, revoked Airwall Edge Services are not displayed in the Conductor. You can display them again by choosing **Revoked** in the **Show All Airwalls** box.

To re-activate a revoked Airwall Edge Service:

1. Log in as an administrator with manager access rights to the overlays the Airwall Edge Service belongs to.
2. Go to the **Airwalls** page.
3. In the **Show all Airwalls** box, select **Revoked**, and find the revoked Airwall Edge Service.
4. Select the arrow to the right of the Airwall Edge Service you want to re-activate.
5. Select **Re-activate** and in the confirmation dialog, click **Apply**.

The Airwall Edge Service is re-activated, and "(revoked)" is removed from its name.



Note: Only System Administrators have permission to re-activate revoked Airwall Edge Services.

Troubleshoot MAP2 Protocol Issues

Conductors and Airwall Gateways running versions 2.0.0 or greater use a new metadata protocol (MAP2). MAP2 allows for better scalability and performance than the previously implemented IF-MAP protocol.



Note: A Conductor running 2.0.x and 2.1.x can also run the legacy IF-MAP protocol to support any Airwall Edge Services running version 1.x.

To help verify the Conductor and Airwall Edge Service are communicating, the Airwall Edge Service maintains the following data:

1. Signature of the Conductor identity
2. The Conductor's shared Airwall Edge Service key

The shared Airwall Edge Service key can be viewed and changed in the Conductor from **Settings > Advanced > Shared HIPservice key**.

If neither of those values match, an Airwall Edge Service will not connect to the Conductor. A factory reset will be required for an Airwall Gateway to connect to a different Conductor.



Note: Beginning in version 2.1.0, the shared key provided to the Airwall Edge Service is now encrypted. If an Airwall Edge Service was previously connected to a 2.0.x Conductor and refuses to connect to a 2.1.x Conductor that has the correct shared key, disabling shared key encryption might help.

You can disable shared key encryption from the Conductor by going to **Settings > Advanced > Disable shared key encryption**.



Note: If you disable shared key encryption, enable it again after all Airwall Edge Services have successfully connected.

Measure wireless signal strength - WiFi and cellular

There are two methods to determine the signal strength of a WiFi-enabled Airwall Gateway.

1. Go to **Airwalls** and select an Airwall Edge Service from the list. Click **Reporting**, where the signal strength is reported every five minutes.

2. Place the Airwall Gateway in diagnostic mode. See [Put an Airwall Gateway into diagnostic mode](#) on page 411 for more information.
3. Once the Airwall Gateway is in diagnostic mode, select **Status** on the diagnostic page.
4. The wireless signal strength is displayed. Refresh the diagnostic mode page to update the signal strength. Signal strength is updated every 5 seconds.

Advisory Notices and Product Bulletins

This section contains important information such as security vulnerabilities, end-of-life notices, and other product updates.

Recent notices and bulletins

- [Software support end of life for versions 2.1.x and earlier](#) on page 422
- [Linux OS End of Support](#) on page 423
- [Platform end-of-life for Airwall Gateway/ HIPswitch 100 series](#) on page 423

For pre-2.1.x advisories and bulletins, please see [pre-2.2.3 Advisory Notices and Product Bulletins](#).

Advisory Notices

The following is a complete list of our active advisory notices.

Upgrade Airwall Gateway 100e or Airwall Gateway 100g to newer firmware

Upgrade Airwall Gateway 100 to version 2.2 may result in a non-functional unit due to drive space issues.

Advisory ID:	Tempered-201910A-001
Version:	2.2
Updated:	10/01/2019

Description

When a Airwall Gateway 100e or 100g unit has been running for an extended period of time, the unit may run out of space on the temporary drive. Before performing an upgrade to the latest firmware, you must reboot the Airwall Gateway prior to installing the firmware update. If this is not done, the Airwall Gateway will not complete the upgrade properly and may result in a non-functional Airwall Gateway.

Affected Products

- Airwall Gateway 100e
- Airwall Gateway 100g

Processor Speculative Execution and Indirect Branch Prediction Vulnerabilities

The Spectre and Meltdown vulnerabilities in modern processor architecture optimizations, allow unprivileged local attackers to read arbitrary memory without restrictions.

Advisory ID:	Tempered-201801A-001
CVEs:	CVE-2017-5715, CVE-2017-5753, CVE-2017-5754
Version:	2.0
Updated:	2/21/2018
Status:	Interim

Overview

Impact

Successful vulnerability exploitation requires the attacker's ability to run code on the targeted machine.

Airwall Gateway & Conductor

Airwall Gateway and Conductor are purpose-built systems that do not allow remote or local system login, execution/installation of arbitrary code, nor the addition of operating system users. This design does not expose them to Spectre and Meltdown attacks.

HIPApps

Airwall Agent and Airwall Server are exposed to Spectre and Meltdown vulnerabilities through the hardware they are installed on. Work with your operating system and hardware vendors to receive the appropriate mitigation software and/or microcode.

Virtual Airwall Gateways & Conductor

Virtualized Airwall Gateway, Virtualized Conductor, and Cloud Airwall Gateway are vulnerable to Spectre and Meltdown through the hypervisor hardware which hosts them. Work with your hypervisor, cloud, and/or hardware vendors to receive the appropriate mitigation software and microcode.

Affected Products

- None directly
- Airwall Agents and Servers and Virtuals via the host hardware

Remediation

- Airwall Gateway and Conductor – none
- Airwall Agents and Servers and Virutals: Mitigation updates for the host operating system and/or hardware microcode

References

- <https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html>
- <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715>
- <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5753>
- <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5754>
- <https://spectreattack.com/>

Product Bulletins

The following is a complete list of our active product bulletins.

For pre-2.1.x advisories and bulletins, please see [pre-2.2.3 Advisory Notices and Product Bulletins](#).

Software support end of life for versions 2.1.x and earlier

Tempered is announcing our intent to end support for software versions 2.1.x and earlier on March 31, 2022.

Platforms:	All platforms
Product versions:	v2.1.x and earlier
Effective date:	March 31, 2022

After the effective date, Tempered will no longer provide troubleshooting services nor develop hot fixes for deployments running v2.1.x or earlier software.

Start planning to update your deployments to the latest Airwall software and firmware releases as soon as possible. For information about update planning, including a recommend update path, see [Manage Versions of Airwall Agents](#)

and Servers on page 106. If you require additional planning assistance, please contact your solution architect or Tempered Customer Success at <https://tempered.force.com/TemperedSupportCenter/s/> or email support@tempered.io.

Linux OS End of Support

Amazon Web Services and Azure cloud providers have announced that they will no longer support Ubuntu16 and Centos7 Linux servers that are reaching the end of support by their providers.

Affected Linux OS Versions

- Ubuntu16
- Centos7

End of Support Date

Mar 31, 2022

Tempered also will no longer support these versions on these cloud platforms after the end of support date. Tempered may continue to support these platforms for non-cloud deployments and for cloud providers that still support them.

For more information, see the announcements from the Linux OS providers.

Platform end-of-life for Airwall Gateway/ HIPswitch 100 series

Tempered announces the End of Life schedule for the Airwall Gateway/HIPswitch 100 series platforms.

End of life schedule for the 100 series

Date	Milestone	Description
10/30/2019	End of Sale	Last date on which the platform may be purchased
5/24/2021	Last supported Software version	The 100 series support v2.2.x software versions. Attempts to install 3.x or later versions will fail.
10/30/2021	Last Full Term MSMU Renewal	Last date a MSMU contract may be renewed for a full 12-month term. MSMU contracts apply only to 300 appliance products with perpetual software licenses. Contracts renewed after this date are required to end no later than 01/01/2022.
10/1/2022	Platform End of Life	Date on which the platform is no longer supported by Tempered.

Multiple-spoke HIPswitch Deployment Tunnel Issues

Hotfix available for tunnel issues in multiple-spoke (over 16) Hub-and-Spoke deployments.

Affected platforms:

HS-150 HS-250 HS-300 HS-400 HS-500

Affected product versions:

2.2.2



Note:

This affects physical, virtual, and cloud Airwall Gateways.

Issue – There is a bug in the HIP tunnel update that can be triggered when you are using Autoconnect and more than 16 spokes on a Hub-and-Spoke deployment. The symptom of this bug is the short-term drop of a HIP tunnel (from 2-3 minutes). This affects a random tunnel or tunnels once every hour.

Solution - Upgrade to 2.2.2, and then download hotfix HF-12219 and apply it to the hub Airwall Gateway of your network.

Download - https://temperedsoftware.s3.amazonaws.com/release/hotfixes/HIPswitch_hotfix-12219

Platform end-of-life for HIPswitch 300 series

Tempered announces the End of Life schedule for HIPswitch 300 series platforms.

End of life schedule for the 300 series

Date	Milestone	Definition
01/01/2019	End of Sale	Last date on which the platform may be purchased
11/13/2019	Last supported Software version	The 300 series support software versions up to v2.1.7. Attempts to install v2.1.8 or later will fail.
01/01/2020	Last Full Term MSMU Renewal	Last date a MSMU contract may be renewed for a full 12 month term. MSMU contracts apply only to the 300 appliance products with perpetual software licenses. Contracts renewed after this date are required to end no later than 01/01/2020.
01/01/2021	Platform End of Life	The date on which the platform is no longer supported by Tempered.

Tempered Networks harmonized tariff codes and country of origin

Affected platforms: All Platforms

Details

Platform Series	HTS Code	Country of Origin
Conductor 500 Series	8517620020	Taiwan
HIPswitch 75 Series	8517620020	China
HIPswitch 100 Series	8517620020	Taiwan
HIPswitch 150 Series (base platform only)	8517620020	China
HIPswitch 150 Series cellular expansion modules	8517620010	China
HIPswitch 250 Series	8517620020	China
HIPswitch 500 Series	8517620020	Taiwan

Software support end of life for versions 1.12.6 and earlier

Affected platforms: All platforms

Affected product versions: 1.12.x and earlier

Date effective: September 16, 2019

Tempered Networks is providing six-month advance notice of our intent to end support for software versions 1.12.6 and earlier on September 16, 2019, the **Effective Date** noted above. After the effective date, Tempered Networks will no longer provide troubleshooting services or develop hot fixes for deployments running 1.12.6 or earlier software. See below for customer resolution.

We strongly recommend that customers start planning to upgrade their deployments to the latest software release as soon as possible. For information about upgrade planning, including a recommended upgrade path, please visit the Tempered Networks Online Documentation here: temperednetworks.com/webhelp. If you require additional planning assistance, please contact your solution architect or Tempered Networks Customer Support at <https://tempered.force.com/TemperedSupportCenter/s/>.

IF-MAP protocol deprecated in IDN 2.2

Affected platforms:

Conductor 400 Conductor 500 Conductor, all cloud platforms Conductor, all virtual platforms

Affected product versions:

1.x and earlier

Conductor software versions 2.1.x and earlier use the IF-MAP protocol to facilitate communication between Conductor and HIP Services running software versions 1.x.x. However, as of Conductor software version 2.2.0, the IF-MAP protocol is no longer supported. Customers applying a version 2.2.0 upgrade to Conductor will experience loss of connectivity with HIP Services running versions earlier than 2.0.0, and need to plan their upgrade path accordingly.

When planning an upgrade of Conductor to version 2.2.0, we strongly recommend that customers verify all HIP Services are running software version 2.1.x or later. For information about upgrade planning, including a recommended upgrade path, please visit the Tempered Networks Online Documentation here: temperednetworks.com/webhelp. If you require additional planning assistance, please contact your solution architect or Tempered Customer Support at <https://tempered.force.com/TemperedSupportCenter/s/>.

Important Patch for HIPswitch-100 and HIPswitch-250 running version 2.1.3

An issue was recently discovered in 2.1.3 when a HIPswitch is in service for a long period of time. When a network interface reaches a total of 2.1GB of traffic, an internal management daemon starts experiencing errors and restarts repeatedly. These restarts appear in the Conductor UI as HIPswitch connects and disconnects. No HIP traffic issues occur when this happens, and secure tunnels will remain intact. The noticeable behavior is the periodic loss of connection to the Conductor.

A hotfix for 2.1.3 is available for the affected platforms. Tempered Networks strongly recommends this hotfix to all customers who have affected platforms running version 2.1.3.

If you are unable to install the hotfix, disable traffic stats reporting for the affected platforms. This action can be performed from the Conductor.

You can download the hotfixes for your platform here or from the [Hotfixes](#) on page 454 page:

- **HIPswitch 100 Series:** [Hotfix 8543](#)
- **HIPswitch 250 Series:** [Hotfix 8551](#)

Important HIPswitch 250 Verizon modem firmware update

Verizon is rolling out an upgrade to their towers that has a known issue with the modem used in the HIPswitch 250.

Our vendor has issued a firmware update for this issue, customers with a HIPswitch 250g or HIPswitch 250gd need to apply this firmware update for compatibility with the Verizon update.

Issue

In rare cases, the module may not be able to attach to an LTE cell in a particular network condition because the module is unable to decode some SIB messages and skip additional information element introduced in higher than 3GPP versions 9.13.0. The module will fallback to 3G if the corresponding cell is available.

Resolution

Update to the newest firmware for the modem.

This firmware is released for Tempered Networks HIPswitch 250g and HIPswitch 250gd connecting to Verizon.

The firmware is available at:

<https://app.box.com/shared/static/7coj9v4ychhel3rlpl8lvzjho2qs6b7y.package>

Airwall API

[resources/api.html](#)

Script Repository

Device Failover

The Conductor API allows for collecting and modifying attributes in Conductor. The following script is an example of how to perform device failover within an overlay network.

Select a device in an overlay and replace it with a different device or device group.

Prerequisites

- Experience with Python and install Python packages
- RESTful API experience
- Conductor user account with API access enabled



Note: ICMP is used to monitor a host to determine when to failover. This requires a sudoer or Administrator account to run.

Required Python Packages

- multiping
- requests



Note: Other imports in this script should be covered by Python's default packages. If not included, you may have to install them manually.

Sample Script

```
#!/usr/bin/python3

from ipaddress import ip_address
import json
from multiping import MultiPing
import os
import requests
from requests.packages.urllib3.exceptions import InsecureRequestWarning
import sys
import time

# Suppress cert warning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

url = "https://<Conductor IP>/api/v1/"

# pre-2.1.3 API headers
# headers = {
#     'x-person-token': '1234',
#     'x-person-email': 'api@temperednetworks.com',
#     'content-type': 'application/json'
# }

headers = {
    'x-api-client-id': 'KWFCITL4VX_B-ZSdywD0Eg',
    'x-api-token': 'grui5TWLvvic8mZ7fgglbA',
```

```

        'content-type': 'application/json'
    }

def generate_menu_select(cont, msg):
    """
    Generate a menu structure from a list of dictionaries

    :param cont: content to be processed
    :param msg: message to be asked

    :returns: selected object from list
    """

    data = sorted(cont, key=lambda k: k['name'])
    for d in data:

        print('{0}) {1}'.format(data.index(d) + 1, d['name']))

    i = input(msg)

    try:
        return data[int(i) - 1]
    except (IndexError, ValueError):
        print('Selected input {0} not found or invalid'.format(i))
        sys.exit()

def get_overlay():
    """
    Get all overlays in Conductor

    :returns: selected overlay network
    """

    r = requests.get(url + "overlay_networks", headers=headers,
verify=False)

    if r.status_code == requests.codes.ok:
        print('Collected overlays:')
        return generate_menu_select(r.json(),
                                      "Select overlay network to failover: ")
    else:
        print('Error getting overlay networks')
        print(r.json())
        sys.exit()

def get_object_in_overlay(devs, dgs, ovl_gps):
    """
    Get all devices/device groups in the overlay. Move to own list.

    :param devs: all devices
    :param dgs: all device groups
    :param ovl_gps: all devices/device groups in overlay

    :returns: selected device/device group
    """

    # devices and device groups
    grps = [d for d in devs for o in ovl_gps if o == d['uuid']]
    grps.extend([d for d in dgs for o in ovl_gps if o == d['uuid']])

    print('Collected devices and device groups in overlay network:')

```

```
    return generate_menu_select(grps, 'Select device/device group to
replace: ')
```

```
def get_device_groups():
    """
    Get all device groups in Conductor
    :returns: all Conductor device groups
    """

    r = requests.get(url + "device_groups", headers=headers, verify=False)

    if r.status_code == requests.codes.ok:
        return r.json()
    else:
        print('Error getting device groups')
        print(r.json())
        sys.exit()
```

```
def get_devices():
    """
    Get all devices in Conductor
    :returns: all Conductor devices
    """

    r = requests.get(url + "devices", headers=headers, verify=False)

    if r.status_code == requests.codes.ok:
        return r.json()
    else:
        print('Error getting devices')
        print(r.json())
        sys.exit()
```

```
def add_device_to_overlay(ovl_uuid, d_uuid):
    """
    Add a device to an overlay network
    :param ovl_uuid: overlay network UUID
    :param d_uuid: device UUID
    """

    payload = {'network_id': ovl_uuid,
               'device_group_ids': [d_uuid]}

    r = requests.post(url + "overlay_network_devices", headers=headers,
                      data=json.dumps(payload), verify=False)

    if not r.status_code == requests.codes.ok:
        print('Error adding to overlay')
        print(r.json())
        sys.exit()
```

```
def remove_device_from_overlay(ovl_uuid, d_uuid):
    """
    Remove a device from an overlay network
    :param ovl_uuid: overlay network UUID
    :param d_uuid: device UUID
```

```

"""
payload = {'network_id': ovl_uuid,
           'device_group_ids': [d_uuid]}

r = requests.delete(url + "overlay_network_devices", headers=headers,
                     data=json.dumps(payload), verify=False)

if not r.status_code == requests.codes.ok:
    print('Error removing from overlay')
    print(r.json())
    sys.exit()

def build_overlay_policy(ovl_uuid, d_uuid, ds_uuid):
    """
    Build the overlay policy

    :param ovl_uuid: overlay network UUID
    :param d_uuid: device UUID
    :param ds_uuid: UUIDs of devices in policy with previous device (target)
    """

    for uuid in ds_uuid:
        payload = {'network_id': ovl_uuid,
                   'device_group_1': d_uuid,
                   'device_group_2': uuid}

        r = requests.post(url + "overlay_network_devices/trust",
                           headers=headers,
                           data=json.dumps(payload), verify=False)

        if not r.status_code == requests.codes.ok:
            print('Error adding policy in overlay')
            print(r.json())

def get_replacement_object(devs, dgs):
    """
    Select which object to use as a replacement

    :param devs: all devices
    :param dgs: all device groups

    :returns: device/device group JSON data
    """

    selection = [{'name': 'Device'}, {'name': 'Device Group'}]

    sel = generate_menu_select(selection, 'Type to replace with: ')

    if sel['name'] == 'Device':
        return generate_menu_select(devs, 'Select replacement device: ')
    elif sel['name'] == 'Device Group':
        return generate_menu_select(dgs, 'Select replacement device group: ')
    )

def replace_overlay_object(ovl, target, replacement):
    """
    Replace a given target with a replacement device/device group object

    :param ovl: overlay JSON data
    :param target: target device JSON data
    """

```

```
:param replacement: replacement device JSON data
"""

policies = [p for p in [t['from'] for t in ovl['policy']] if t['to'] == target['uuid']]

remove_device_from_overlay(ovl['uuid'], target['uuid'])
print('Removing device from overlay')
add_device_to_overlay(ovl['uuid'], replacement['uuid'])
print('Adding replacement device to overlay')
build_overlay_policy(ovl['uuid'], replacement['uuid'], policies)
print('Build overlay policy with replacement device')

def select_mon_target():
    """
    Input an IP to monitor
    :returns: IP address to monitor
    """

    selection = True
    mon_target = None

    while selection:
        mon_target = input('Enter IP target to monitor: ')
        try:
            ip_address(mon_target)
            selection = False
        except ValueError:
            print('Invalid IP address.')
            continue

    return mon_target

def monitor_target(mon_target):
    """
    Monitor the given target import ip
    :param mon_target: IP address to monitor
    """

    active = True
    while active:
        if mon_target:
            mp = MultiPing([mon_target])
            mp.send()
            resp, no_resp = mp.receive(.1)
            stamp = time.strftime('%Y-%m-%d %H:%M:%S')

            if no_resp:
                print('{0}: Monitor failed'.format(stamp))
                break
            else:
                print('{0}: Ping monitor successful'.format(stamp))
                time.sleep(1)

def main():

    if not os.geteuid() == 0:
        print('Must run as root or Administrator. Exiting...')
```

```

else:

    # get content
    ovl = get_overlay()
    devs = get_devices()
    dgs = get_device_groups()

    # ask questions
    target = get_object_in_overlay(devs, dgs, ovl['device_groups'])
    replacement = get_replacement_object(devs, dgs)

    # monitor ip
    mon_target = select_mon_target()
    monitor_target(mon_target)

    # do work
    replace_overlay_object(ovl, target, replacement)
    print('Device failover completed')

if __name__ == "__main__":
    try:
        main()
    except KeyboardInterrupt:
        sys.exit()

```

Tempered Software Downloads and Release Notes

Download Tempered's Airwall software and firmware for your version and platform here, and get the release notes for those versions.

For help applying updates, see the following topics:

- [Update Conductor Firmware](#) on page 106
- [Update Airwall Gateway firmware](#) on page 109
- [Update firmware for a group of Airwall Edge Services](#) on page 110

Latest firmware and software

Please follow the links below to download the latest firmware and software. The latest version for each is listed in the download link. For release notes, see [Latest Release Notes \(v3.0\)](#) on page 457:

Conductor firmware

Link	Applies To	File Name
Download 3.0.0	Conductor - All Platforms	Conductor_r2.2.13-1575_package

Airwall firmware

Link	Applies To	File Name
Download 3.0.0	Advantech Airwall Gateway AV3200g installer	temperedfw-r3.0.0-1456.tgz

Link	Applies To	File Name
Download 3.0.0	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r3.0.0-1319_package
Download 3.0.0	Airwall mvebu (All 110-, 150-, and 250-series Airwall Gateways)	Airwall-mvebu_r3.0.0-1456_package
Download 3.0.0	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r3.0.0-1689_package
Download 3.0.0	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r3.0.0-1689-combined-ext4.ova
Download 3.0.0	Airwall Gateway x86_64 Hyper-V image	Airwall-x86_64_r3.0.0-1689-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Link	Applies To	File Name
Airwall Agents		
Download 3.0.0	macOS, OSX Airwall Agent	Airwall-Mac_3.0.0.2065.pkg
Download 2.2.12	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.12.353_Installer.exe
Download 2.2.12	Windows 64 Airwall Agent Express Install	AirwallAgent64-bit_2.2.12.353_ExpressInstaller.exe
Download 2.2.12	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.12.353.msi
Airwall Servers		
Download 3.0.0	Linux/Ubuntu v16 Airwall Server	airwall-ubuntu16_3.0.0-1206_amd64.deb
Download 3.0.0	Linux/Ubuntu v18 and v20 Airwall Server	airwall-ubuntu18_3.0.0-1094_amd64.deb
Download 3.0.0	Linux/CentOS 8 Airwall Server	airwall-3.0.0-819.el8.x86_64.rpm
Download 3.0.0	Linux/CentOS 7 Airwall Server	airwall-3.0.0-1173.el7.x86_64.rpm
Download 3.0.0	Linux/Fedora Airwall Server	airwall-3.0.0-877.fc33.x86_64.rpm
Download 2.2.12	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.12.353_Installer.exe
Download 2.2.12	Windows Server 64 Airwall Server Express Install	AirwallServer64-bit_2.2.12.353_ExpressInstaller.exe
Download 2.2.12	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.12.353.msi

Cellular Modem Firmware Updates

Link	Applies To	File Name
Download	Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package

Link	Applies To	File Name
Download	Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Download	Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Link	Applies To	File Name
Windows, 32-bit	Pre-2.2.3 Airwall Gateway 150 only	
Download Dec 2020	Windows, 64-bit Airwall Gateway 100, 110, and 150	Airwall1XXSerialDriver_x64.msi

3.0 firmware and software

Please follow the links below to download the v3.0 firmware and software. For release notes, see [Release Notes v3.0.0](#) on page 469.



Note: Also review [Hotfixes](#) on page 454 for any hotfix releases.

Checksums

[MD5](#)

[SHA1](#)

Conductor firmware

Link	Applies To	File Name
Download 3.0.0	Conductor - All Platforms	Conductor_r3.0.0-1721_package

Airwall Gateway firmware

Link	Applies To	File Name
Download 3.0.0	Advantech Airwall Gateway AV3200g installer	temperedfw-r3.0.0-1456.tgz
Download 3.0.0	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r3.0.0-1319_package
Download 3.0.0	Airwall mvebu (All 110-, 150-, and 250-series Airwall Gateways)	Airwall-mvebu_r3.0.0-1456_package
Download 3.0.0	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r3.0.0-1689_package
Download 3.0.0	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r3.0.0-1689-combined-ext4.ova
Download 3.0.0	Airwall Gateway x86_64 Hyper-V image	Airwall-x86_64_r3.0.0-1689-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Link	Applies To	File Name
Airwall Agents		
Download 3.0.0	macOS, OSX Airwall Agent	Airwall-Mac_3.0.0.2065.pkg
Download 3.0.0	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.11.333_Installer.exe
Download 2.2.11	Windows 64 Airwall Agent Express Install	AirwallAgent64-bit_2.2.11.333_ExpressInstaller.exe
Download 2.2.11	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi
Airwall Servers		
Download 3.0.0	Linux/Ubuntu v16 Airwall Server	airwall-ubuntu16_3.0.0-1206_amd64.deb
Download 3.0.0	Linux/Ubuntu v18 and v20 Airwall Server	airwall-ubuntu18_3.0.0-1094_amd64.deb
Download 3.0.0	Linux/CentOS 8 Airwall Server	airwall-3.0.0-819.el8.x86_64.rpm
Download 3.0.0	Linux/CentOS 7 Airwall Server	airwall-3.0.0-1173.el7.x86_64.rpm
Download 3.0.0	Linux/Fedora Airwall Server	airwall-3.0.0-877.fc33.x86_64.rpm
Download 2.2.11	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.11.333_Installer.exe
Download 2.2.11	Windows Server 64 Airwall Server Express Install	AirwallServer64-bit_2.2.11.333_ExpressInstaller.exe
Download 2.2.11	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.11.333.msi

Cellular Modem Firmware Updates

Link	Applies To	File Name
Download	Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Download	Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Download	Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 64-bit Airwall 100, 110, and 150	Airwall1XXSerialDriver_x64.msi

2.2.13 firmware and software

Please follow the links below to download the 2.2.13 firmware and software. For release notes, see [Release Notes 2.2.13](#) on page 481.



Note: Also review [Hotfixes](#) on page 454 for any hotfix releases.

Conductor firmware

Link	Applies To	File Name
Download 2.2.13	Conductor - All Platforms	Conductor_r2.2.13-1575_package

Airwall Gateway firmware

Link	Applies To	File Name
Download 2.2.13	Advantech Airwall Gateway AV3200g installer	tempered-advantech-installer-2.2.13.tgz

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Link	Applies To	File Name
Airwall Agents		
Download 2.2.12	macOS, OSX Airwall Agent	Airwall-Mac_2.2.12.1840.pkg
Download 2.2.11	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.11.333_Installer.exe
Download 2.2.11	Windows 64 Airwall Agent Express Install	AirwallAgent64-bit_2.2.11.333_ExpressInstaller.exe
Download 2.2.11	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi
Airwall Servers		
Download 2.2.11	Linux/Ubuntu v16 Airwall Server	airwall-2.2.11.Ubuntu16.amd64.deb
Download 2.2.11	Linux/Ubuntu v18 and v20 Airwall Server	airwall-2.2.11.Ubuntu18.amd64.deb
Download 2.2.11	Linux/CentOS 8 Airwall Server	airwall-2.2.11.Centos8.x86_64.rpm
Download 2.2.11	Linux/CentOS 7 Airwall Server	airwall-2.2.11.Centos7.x86_64.rpm
Download 2.2.11	Linux/Fedora Airwall Server	airwall-2.2.11.Fedora33.x86_64.rpm
Download 2.2.11	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.11.333_Installer.exe
Download 2.2.11	Windows Server 64 Airwall Server Express Install	AirwallServer64-bit_2.2.11.333_ExpressInstaller.exe
Download 2.2.11	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.11.333.msi

Cellular Modem Firmware Updates

Link	Applies To	File Name
Download	Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Download	Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Download	Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 64-bit Airwall 100, 110, and 150	Airwall1XXSerialDriver_x64.msi

2.2.12 firmware and software

Please follow the links below to download the 2.2.12 firmware and software. For release notes, see [Release Notes 2.2.12](#) on page 489.



Note: Also review [Hotfixes](#) on page 454 for any hotfix releases.

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.12-1506_package

Airwall Gateway firmware

Link	Applies To	File Name
Download 2.2.12	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.12-1143_package
Download 2.2.12	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.12-1218_package
Download 2.2.12	Airwall mvebu (All 110-, 150-, and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.12-1272_package
Download 2.2.12	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.12-1482_package
Download 2.2.12	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.12-1482-combined-ext4.ova
Download 2.2.12	Airwall Gateway x86_64 Hyper-V image	Airwall-x86_64_r2.2.12-1482-combined-ext4.vhdx

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.



Note: Linux Airwall Agents and Servers are not part of the v2.2.12 release. Use v2.2.11 available at [Latest firmware and software](#) on page 431.

Link	Applies To	File Name
Airwall Agents		
Download 2.2.12	macOS, OSX Airwall Agent	Airwall-Mac_2.2.12.1977.pkg
Download 2.2.12	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.12.353_Installer.exe

Link	Applies To	File Name
Download 2.2.12	Windows 64 Airwall Agent Express Install	AirwallAgent64-bit_2.2.12.353_ExpressInstaller.exe
Download 2.2.12	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.12.353.msi
Airwall Servers		
Download 2.2.11	Linux/Ubuntu v16 Airwall Server	airwall-2.2.11.Ubuntu16.amd64.deb
Download 2.2.11	Linux/Ubuntu v18 and v20 Airwall Server	airwall-2.2.11.Ubuntu18.amd64.deb
Download 2.2.11	Linux/CentOS 8 Airwall Server	airwall-2.2.11.Centos8.x86_64.rpm
Download 2.2.11	Linux/CentOS 7 Airwall Server	airwall-2.2.11.Centos7.x86_64.rpm
Download 2.2.11	Linux/Fedora Airwall Server	airwall-2.2.11.Fedora33.x86_64.rpm
Download 2.2.12	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.12.353_Installer.exe
Download 2.2.12	Windows Server 64 Airwall Server Express Install	AirwallServer64-bit_2.2.12.353_ExpressInstaller.exe
Download 2.2.12	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.12.353.msi

Cellular Modem Firmware Updates

Link	Applies To	File Name
Download	Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Download	Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Download	Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 64-bit Airwall 100, 110, and 150	Airwall1XXSerialDriver_x64.msi

2.2.11 firmware and software

Please follow the links below to download the 2.2.11 firmware and software. For release notes, see [Release Notes 2.2.11](#) on page 502.



Note: Also review [Hotfixes](#) on page 454 for any hotfix releases.

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.11-1432_package

Airwall Gateway firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.11-1053_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.11-1126_package
Download	Airwall mvebu (All 110-, 150-, and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.11-1179_package
Download	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.11-1390_package
Download	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.11-1390-combined-ext4.ova
Download	Airwall Gateway x86_64 Hyper-V image	Airwall-x86_64_r2.2.11-1390-combined-ext4.vhdx

Airwall Agents and Servers Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Link	Applies To	File Name
Airwall Agents		
Download 2.2.11	macOS, OSX Airwall Agent	Airwall-Mac_2.2.11.1775.pkg
Download 2.2.11	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.11.333_Installer.exe
Download 2.2.11	Windows 64 Airwall Agent Express Install	AirwallAgent64-bit_2.2.11.333_ExpressInstaller.exe
Download 2.2.11	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.11.333.msi
Airwall Servers		
Download 2.2.11	Linux/Ubuntu v16 Airwall Server	airwall-2.2.11.Ubuntu16.amd64.deb
Download 2.2.11	Linux/Ubuntu v18 and v20 Airwall Server	airwall-2.2.11.Ubuntu18.amd64.deb
Download 2.2.11	Linux/CentOS 8 Airwall Server	airwall-2.2.11.Centos8.x86_64.rpm
Download 2.2.11	Linux/CentOS 7 Airwall Server	airwall-2.2.11.Centos7.x86_64.rpm
Download 2.2.11	Linux/Fedora Airwall Server	airwall-2.2.11.Fedora33.x86_64.rpm
Download 2.2.11	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.11.333_Installer.exe
Download 2.2.11	Windows Server 64 Airwall Server Express Install	AirwallServer64-bit_2.2.11.333_ExpressInstaller.exe
Download 2.2.11	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.11.333.msi

Cellular Modem Firmware Updates

Link	Applies To	File Name
Download	Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Download	Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Download	Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 64-bit Airwall 100, 110, and 150	Airwall1XXSerialDriver_x64.msi

2.2.10 firmware and software

Please follow the links below to download the 2.2.10 firmware and software. For release notes, see [Release Notes 2.2.10](#) on page 516.



Note: Also review [Hotfixes](#) on page 454 for any hotfix releases.

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.10-1286_package

Airwall Gateway firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.10-921_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.10-999_package
Download	Airwall mvebu (All 110-, 150-, and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.10-1065_package
Download	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.10-1251_package
Download	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.10-1251-combined-ext4.ova

Airwall Agents and Servers Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Link	Applies To	File Name
Airwall Agents		
Download 2.2.10	macOS, OSX Airwall Agent	Airwall-Mac-2.2.10-1594-signed.pkg

Link	Applies To	File Name
Download 2.2.10	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.10_Installer.exe
Download 2.2.10	Windows 64 Airwall Agent Express Install	AirwallAgent64-bit_2.2.10_ExpressInstaller.exe
Download 2.2.10	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.10.msi
Airwall Servers		
Download 2.2.10	Linux/Ubuntu v16 Airwall Server	airwall-2.2.10.Ubuntu16.amd64.deb
Download 2.2.10	Linux/Ubuntu v18 and v20 Airwall Server	airwall-2.2.10.Ubuntu18.amd64.deb
Download 2.2.10	Linux/CentOS 8 Airwall Server	airwall-2.2.10.Centos8.x86_64.rpm
Download 2.2.10	Linux/CentOS 7 Airwall Server	airwall-2.2.10.Centos7.x86_64.rpm
Download 2.2.10	Linux/Fedora 2.7 Airwall Server	airwall-2.2.10.Fedora27.x86_64.rpm
Download 2.2.10	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.10_Installer.exe
Download 2.2.10	Windows Server 64 Airwall Server Express Install	AirwallServer64-bit_2.2.10_ExpressInstaller.exe
Download 2.2.10	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.10.msi

Cellular Modem Firmware Updates

Link	Applies To	File Name
Download	Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Download	Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Download	Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 64-bit Airwall 100, 110, and 150	Airwall1XXSerialDriver_x64.msi

2.2.8 firmware and software

Please follow the links below to download the 2.2.8 firmware and software. For release notes, see [Release Notes 2.2.8](#) on page 537.



Note: Also review [Hotfixes](#) on page 454 for any hotfix releases.

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.8-1102_package

Airwall firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.8-767_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.8-846_package
Download	Airwall mvebu (All 150-series and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.8-863_package
Download	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.8-1043_package
Download	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.8-1043-combined-ext4.ova

Airwall Agent and Airwall Server Software

For the latest iOS and Android Airwall Agents, search for "Airwall Agent" in the store for your device.

Link	Applies To	File Name
Airwall Agents		
Download 2.2.8 update	macOS, OSX Airwall Agent	Airwall-Mac-2.2.8-signed.pkg
Download 2.2.8 update	Windows 64 Airwall Agent Install	AirwallAgent64-bit_2.2.8_Installer.exe
Download 2.2.8 update	Windows 64 Airwall Agent Express Install	AirwallAgent64_ExpressInstaller_2.2.8.exe
Download 2.2.8 update	Windows 64 Unattended Install	AirwallAgent64-bit_UnattendedInstaller_2.2.8.msi
Airwall Servers		
Download 2.2.8 update	Linux/Ubuntu v16 Airwall Server	airwall-ubuntu16_2.2.8_amd64.deb
Download 2.2.8 update	Linux/Ubuntu v18 and v20 Airwall Server	airwall-ubuntu18_2.2.8_amd64.deb
Download 2.2.8 update	Linux/CentOS 8 Airwall Server	airwall-Centos8_2.2.8_x86_64.rpm
Download 2.2.8 update	Linux/CentOS 7 Airwall Server	airwall-Centos7_2.2.8_x86_64.rpm
Download 2.2.8 update	Linux/Fedora 2.7 Airwall Server	airwall-Fedora27_2.2.8_x86_64.rpm
Download 2.2.8 update	Windows Server 64 Airwall Server Install	AirwallServer64-bit_2.2.8_Installer.exe
Download 2.2.8 update	Windows Server 64 Airwall Server Express Install	AirwallServer64_2.2.8_ExpressInstaller.exe
Download 2.2.8 update	Windows Server 64 Airwall Server Unattended Install	AirwallServer64-bit_UnattendedInstaller_2.2.8.msi

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 32-bit Airwall 150	HIPswitch150Driver_x86.msi
Download	Windows, 64-bit Airwall 150	HIPswitch150Driver_x64.msi

2.2.5 firmware and software

Please follow the links below to download the 2.2.5 firmware and software. For release notes, see [Release Notes 2.2.5](#) on page 551:

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.5-907_package

Airwall firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.5-630_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.5-711_package
Download	Airwall mvebu (All 150-series and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.5-731_package
Download	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.5-890_package
Download	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.5-890-combined-ext4.ova

Airwall Agent and Airwall Server Software

Link	Applies To	File Name
Airwall Agents		
Download	macOS, OSX Airwall Agent	Airwall-Mac-2.2.3-1270-signed.pkg

Link	Applies To	File Name
Download	Windows 64 Airwall Agent Install	AirwallClient64_2.2.3.620_20200218_Installer.exe
Download	Windows 64 Airwall Agent Express Install	AirwallClient64_2.2.3.648_ExpressInstaller.exe
Download	Windows 64 Unattended Install	AirwallClient64_UnattendedInstaller_2.2.3.msi
Download	Windows 64 Airwall Agent Upgrade Package (2.2.2 to 2.2.3 only)	Airwall-Winclient_64_r2.2.3-620_package
Airwall Servers		
Download	Linux/Ubuntu v16 Airwall Server	airwall-ubuntu16_2.2.3-469_amd64.deb
Download	Linux/Ubuntu v18 Airwall Server	airwall-ubuntu18_2.2.3-377_amd64.deb
Download	Linux/CentOS 8 Airwall Server	airwall-2.2.3-124.el8.x86_64.rpm
Download	Linux/CentOS 7 Airwall Server	airwall-2.2.3-449.el7.x86_64.rpm
Download	Linux/Fedora 2.7 Airwall Server	airwall-2.2.3-151.fc27.x86_64.rpm
Download	Windows Server 64 Airwall Server Install	AirwallServer64_2.2.3.623_20200218_Installer.exe
Download	Windows Server 64 Airwall Server Express Install	AirwallServer64_2.2.3.651_ExpressInstaller.exe
Download	Windows Server 64 Airwall Server Unattended Install	AirwallServer64_UnattendedInstaller_2.2.3.msi
Download	Windows 64 Airwall Server Upgrade Package (2.2.2 to 2.2.3 only)	Airwall-Winserver_64_r2.2.3-623_package

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	Windows, 32-bit Airwall 150	HIPswitch150Driver_x86.msi
Download	Windows, 64-bit Airwall 150	HIPswitch150Driver_x64.msi

2.2.3 firmware and software

Please follow the links below to download the 2.2.3 firmware and software. For release notes, see [Release Notes 2.2.3](#) on page 554:

Conductor firmware

Link	Applies To	File Name
Download	Conductor - All Platforms	Conductor_r2.2.3-805_package

Airwall firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series)	Airwall-mvebu64_r2.2.3-546_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	Airwall-ramips_r2.2.3-629_package
Download	Airwall mvebu (All 150-series and 250-series Airwall Gateways)	Airwall-mvebu_r2.2.3-648_package
Download	Airwall x86_64 (100rc, virtual 300-series, 400-series, and 500-series Airwall Gateways)	Airwall-x86_64_r2.2.3-802_package
Download	Airwall x86_64 OVA (ESXi)	Airwall-x86_64_r2.2.3-802-combined-ext4.ova

Airwall Agent and Airwall Server Software

Link	Applies To	File Name
Airwall Agents		
Download	macOS, OSX Airwall Agent	Airwall-Mac-2.2.3-signed.pkg
Download	Windows 64 Airwall Agent Install	AirwallClient64_2.2.3_Installer.exe
Download	Windows 64 Airwall Agent Express Install	AirwallClient64_ExpressInstaller_2.2.3.exe
Download	Windows 64 Unattended Install	AirwallClient64_UnattendedInstaller_2.2.3.msi
Download	Windows 64 Airwall Agent Upgrade Package (2.2.2 to 2.2.3 only)	Airwall-Winclient_64_r2.2.3_package
Airwall Servers		
Download	Linux/Ubuntu v16 Airwall Server	airwall-ubuntu16_2.2.3_amd64.deb
Download	Linux/Ubuntu v18 Airwall Server	airwall-ubuntu18_2.2.3_amd64.deb
Download	Linux/CentOS 8 Airwall Server	airwall-2.2.3.el8.x86_64.rpm
Download	Linux/CentOS 7 Airwall Server	airwall-2.2.3.el7.x86_64.rpm
Download	Linux/Fedora 2.7 Airwall Server	airwall-2.2.3.fc27.x86_64.rpm
Download	Windows Server 64 Airwall Server Install	AirwallServer64_2.2.3_Installer.exe
Download	Windows Server 64 Airwall Server Express Install	AirwallServer64_2.2.3_ExpressInstaller.exe
Download	Windows Server 64 Airwall Server Unattended Install	AirwallServer64_UnattendedInstaller_2.2.3.msi

Link	Applies To	File Name
Download	Windows 64 Airwall Server Upgrade Package (2.2.2 to 2.2.3 only)	Airwall-Winserver_64_r2.2.3_package

Cellular modem firmware

Firmware updated Dec 16, 2020

Please follow the links below to download firmware:

Checksums: [MD5 SHA-1](#)

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download	Airwall Gateway 110	Airwall-110_cellfw-9224c85-106_package
Download	Airwall Gateway 150	Airwall-150_cellfw-9224c85-106_package
Download	Airwall Gateway 250	Airwall-250_cellfw-9224c85-106_package

Serial drivers

64-bit drivers updated Dec 16, 2020

Please follow the links below to download serial drivers for your Airwall Gateway. If you need instructions for accessing the Airwall Gateway via the console port, see [Connecting to the console port on an Airwall Gateway](#) on page 250.

Checksums: [MD5 SHA-1](#)

Airwall 75

The PL2303 Chip is built into the Airwall 75 to provide serial connectivity to the console. However, the driver is not included out-of-the-box with Windows or macOS, so you need to download it from the manufacturer's site and install it before you connect.

Download: [Windows](#) | [macOS](#)

Airwall 110 and 150

A custom chip built into these Airwall Gateways provides serial connectivity to the console. This chip has drivers for Linux and macOS built-in, but Windows requires you to download and install a driver before you can connect.

Download:

- Windows, 32-bit – Available on request (contact Customer Success at support@tempered.io).
- [Windows, 64-bit](#) – 110 or 150 (Dec 2020 update)

Airwall 250

The FT232RL chip is built into the Airwall 250 to provide serial connectivity to the console. However, this driver is not included out-of-the-box with Windows or OSX/macOS, so you need to download it before you connect.

Download: [All platforms](#)

Older downloads

Downloads for 2.1.x to 2.2.2 firmware and software versions. For firmware downloads for versions 1.12.1 through 2.0.x, see the [pre-2.2.3 software downloads page](#).

2.2.2 firmware and software

Please follow the links below to download version 2.2.2 firmware:

Checksums:

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.2.2-587_package
Download	Conductor, Azure	Conductor-azure_r2.2.2-587_package

HIPswitch firmware

Link	Applies To	File Name
Download	HIPswitch mvebu64 (All 75-series HIPswitches)	HIPswitch-mvebu64_r2.2.2-394_package
Download	HIPswitch ramips (100g and 100e HIPswitches)	HIPswitch-ramips_r2.2.2-480_package
Download	HIPswitch mvebu (All 150-series and 250-series HIPswitches)	HIPswitch-mvebu_r2.2.2-483_package
Download	HIPswitch x86_64 (100rc, virtual 300-series, 400-series, and 500-series HIPswitches)	HIPswitch-x86_64_r2.2.2-594_package
Download	HIPswitch x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.2.2-598-combined-ext4.ova
Download	HIPswitch x86_64 (Azure)	HIPswitch-x86_64-azure_r2.2.2-598_package

Software

Link	Applies To	File Name
Download	HIPclient (OSX, macOS)	HIPclient_2.2.1.924.pkg
Download	HIPclient (Windows 32) Express Install	HIPclient32_2.2.2.378_ExpressInstaller.exe
Download	HIPclient (Windows 64) Express Install	HIPclient64_2.2.2.432_ExpressInstaller.exe
Download	HIPserver (Linux/Ubuntu v16)	hipserver_2.2.2-307_amd64.deb
Download	HIPserver (Linux/Ubuntu v18)	hipserver_2.2.2-213_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver-2.2.2-291.el7.x86_64.rpm

Link	Applies To	File Name
Download	HIPserver (Windows Server 64) Express Install	HIPserver64_2.2.2.443_ExpressInstaller.exe

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	HIPswitch 150 (Windows, 32-bit)	HIPswitch150Driver_x86.msi
Download	HIPswitch 150 (Windows, 64-bit)	HIPswitch150Driver_x64.msi

2.2.1 firmware and software

Please follow the links below to download version 2.2.1 firmware:

Checksums:

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.2.1-466_package
Download	Conductor, Azure	Conductor-azure_r2.2.1-466_package

HIPswitch firmware

Link	Applies To	File Name
Download	HIPswitch mvebu64 (All 75-series HIPswitches)	HIPswitch-mvebu64_r2.2.1-294_package
Download	HIPswitch ramips (100g and 100e HIPswitches)	HIPswitch-ramips_r2.2.1-390_package
Download	HIPswitch mvebu (All 150-series and 250-series HIPswitches)	HIPswitch-mvebu_r2.2.1-391_package
Download	HIPswitch x86_64 (100rc, virtual 300-series, 400-series, and 500-series HIPswitches)	HIPswitch-x86_64_r2.2.1-479_package
Download	HIPswitch x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.2.1-479-combined-ext4.ova

Link	Applies To	File Name
Download	HIPswitch x86_64 (Azure)	HIPswitch-x86_64-azure_r2.2.1-479_package
Download	HIPswitch x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.2.1-479-combined-ext4.vhd

Software

Link	Applies To	File Name
Download	HIPclient (Windows, 32-bit)	HIPclient32_2.2.1_Installer.exe
Download	HIPclient (Windows, 32-bit), Unattended Install	HIPclient32_UnattendedInstaller_2.2.1.msi
Download	HIPclient (Windows, 32-bit), Express Install	HIPclient32_2.2.1_ExpressInstaller.exe
Download	HIPclient (Windows, 64-bit)	HIPclient64_2.2.1_Installer.exe
Download	HIPclient (Windows, 64-bit), Unattended Install	HIPclient64_UnattendedInstaller_2.2.1.msi
Download	HIPclient (Windows, 64-bit), Express Install	HIPclient64_2.2.1_ExpressInstaller.exe
Download	HIPserver (Windows, 64-bit)	HIPserver64_2.2.1_Installer.exe
Download	HIPserver (Windows, 64-bit), Unattended Install	HIPserver64_UnattendedInstaller_2.2.1.msi
Download	HIPserver (Windows, 64-bit), Express Install	HIPserver64_2.2.1_ExpressInstaller.exe
Download	HIPclient (OSX, macOS)	HIPclient_2.2.1.pkg
Download	HIPserver (Linux/Ubuntu v16)	hipserver_Ubuntu16-2.2.1_amd64.deb
Download	HIPserver (Linux/Ubuntu v18)	hipserver_Ubuntu18-2.2.1_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver_Centos7-2.2.1_x86_64.rpm

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	HIPswitch 150 (Windows, 32-bit)	HIPswitch150Driver_x86.msi
Download	HIPswitch 150 (Windows, 64-bit)	HIPswitch150Driver_x64.msi

2.1.7 firmware and software

Please follow the links below to download version 2.1.7 firmware:

Checksums: [MD5 SHA-1](#)

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.1.7-1308_package

HIPswitch firmware

Link	Applies To	File Name
Download	HIPswitch mvebu64 (All 75-series HIPswitches)	HIPswitch-mvebu64_r2.1.7-628_package
Download	HIPswitch ramips (100g and 100e HIPswitches)	HIPswitch-ramips_r2.1.7-1095_package
Download	HIPswitch mvebu (All 150-series and 250-series HIPswitches)	HIPswitch-mvebu_r2.1.7-1250_package
Download	HIPswitch x86_64 (100rc, all 300-series, 400-series, and 500-series HIPswitches)	HIPswitch-x86_64_r2.1.7-1512_package
Download	HIPswitch x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.1.7-1523-combined-ext4.ova
Download	HIPswitch x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.1.7-1523-combined-ext4.vhdx

Software



Note: In this maintainence release, our HIP clients and HIP servers remain unchanged from version 2.1.6.

Link	Applies To	File Name
Download	HIPclient (Windows, 32-bit)	HIPclient32_2.1.6.326_20190222_Installer.exe
Download	HIPclient (Windows, 64-bit)	HIPclient64_2.1.6.636_20190222_Installer.exe
Download	HIPserver (Windows, 32-bit)	HIPserver32_2.1.6.250_20190301_Installer.exe
Download	HIPserver (Windows, 64-bit)	HIPserver64_2.1.6.804_20190301_Installer.exe
Download	HIPclient (OSX, macOS)	HIPclient_2.1.6.1209.pkg
Download	HIPserver (Linux/Ubuntu)	hipserver_2.1.6-1007_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver-2.1.6-805.el7.x86_64.rpm

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package

Link	Applies To	File Name
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	HIPswitch 150 (Windows, 32-bit)	HIPswitch150Driver_x86.msi
Download	HIPswitch 150 (Windows, 64-bit)	HIPswitch150Driver_x64.msi

2.1.6 firmware and software

Please follow the links below to download version 2.1.6 firmware:

Checksums: [MD5 SHA-1](#)

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.1.6-1144_package
Download	Conductor, Azure	Conductor_r2.1.6-752-azure_package

HIPswitch firmware

Link	Applies To	File Name
Download	HIPswitch mvebu64 (All 75-series HIPswitches)	HIPswitch-mvebu64_r2.1.6-472_package
Download	HIPswitch ramips (100g and 100e HIPswitches)	HIPswitch-ramips_r2.1.6-941_package
Download	HIPswitch mvebu (All 150-series and 250-series HIPswitches)	HIPswitch-mvebu_r2.1.6-1070_package
Download	HIPswitch x86_64 (100rc, all 300-series, 400-series, and 500-series HIPswitches)	HIPswitch-x86_64_r2.1.6-1357_package
Download	HIPswitch x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.1.6-1357-combined-ext4.ova
Download	HIPswitch x86_64 (Azure)	HIPswitch-x86_64_r2.1.6-781-azure_package
Download	HIPswitch x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.1.6-1357-combined-ext4.vhd

Software

Link	Applies To	File Name
Download	HIPclient (Windows, 32-bit)	HIPclient32_2.1.6_Installer.exe
Download	HIPclient (Windows, 64-bit)	HIPclient64_2.1.6_Installer.exe
Download	HIPserver (Windows, 32-bit)	HIPserver32_2.1.6_Installer.exe
Download	HIPserver (Windows, 64-bit)	HIPserver64_2.1.6_Installer.exe
Download	HIPclient (OSX, macOS)	HIPclient_2.1.6.pkg
Download	HIPserver (Linux/Ubuntu)	hipserver_2.1.6_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver-2.1.6-805.el7.x86_64.rpm

Cellular Modem Firmware Upgrades

Link	Applies To	File Name
Download		HIPswitch-150_cellfw-12ddb86-r12_package
Download		HIPswitch-250_cellfw-12ddb86-r2_package
Download		HIPswitch-250_cellfw-12ddb86-r1_package

Windows Serial Port Drivers

Link	Applies To	File Name
Download	HIPswitch 150 (Windows, 32-bit)	HIPswitch150Driver_x86.msi
Download	HIPswitch 150 (Windows, 64-bit)	HIPswitch150Driver_x64.msi

2.1.5 firmware and software

Please follow the links below to download version 2.1.5 firmware:

Checksums: [MD5](#) [SHA-1](#)

Conductor firmware

Link	Applies To	File Name
Download	Conductor (All Platforms)	Conductor_r2.1.5-1035_package
Download	Conductor, Azure	Conductor_r2.1.5-660-azure_package

Airwall Gateway firmware

Link	Applies To	File Name
Download	Airwall mvebu64 (All 75-series Airwall Gateways)	HIPswitch-mvebu64_r2.1.5-372_package
Download	Airwall ramips (100g and 100e Airwall Gateways)	HIPswitch-ramips_r2.1.5-840_package

Link	Applies To	File Name
Download	Airwall mvebu (All 150-series and 250-series Airwall Gateways)	HIPswitch-mvebu_r2.1.5-972_package
Download	Airwall x86_64 (100rc, all 300-series, 400-series, and 500-series Airwall Gateways)	HIPswitch-x86_64_r2.1.5-1249_package
Download	Airwall x86_64 (Azure)	HIPswitch-x86_64_r2.1.5-687-azure_package
Download	Airwall x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.1.5-1249-combined-ext4.ova
Download	Airwall x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.1.5-1249-combined-ext4.vhd

Software

Link	Applies To	File Name
Download	HIPclient (Windows, 64-bit)	HIPclient64_2.1.5.537_20181212_Installer.exe
Download	HIPclient (Windows, 32-bit)	HIPclient32_2.1.5.240_20181212_Installer.exe
Download	HIPserver (Windows, 64-bit)	HIPserver64_2.1.5.706_20181212_Installer.exe
Download	HIPserver (Windows, 32-bit)	HIPserver32_2.1.5.154_20181212_Installer.exe
Download	HIPclient (OSX, macOS)	HIPclient_2.1.5.1119.pkg
Download	HIPserver (Linux/Ubuntu)	hipserver_2.1.5-922_amd64.deb
Download	HIPserver (Linux/CentOS)	hipserver-2.1.5-720.el7.x86_64.rpm

2.1.4 firmware and software

Please follow the links below to download version 2.1.4 firmware:

Conductor firmware

Link	Applies To	File Name	File Size	Checksum
Download	Conductor (All Platforms, Azure see below)	Conductor_r2.1.4-954_108612787	108612787	MD5: 7a6e0c14fc3b68ff5f2291- SHA 1: f938cb958ab7d2bb2d68d
Download	Conductor, Azure	Conductor_r2.1.4-585-113228503	113228503	MD5: 846221fbecccb8021bab9- SHA-1: 6ebe7af9b51a076c90e08

Airwall Gateway firmware

Link	Applies To	File Name	File Size	Checksum
Download	Airwall mvebu64 (All 75-series Airwall Gateways)	HIPswitch-mvebu64_r2.1.4-305_package	27864195	MD5: 6c0c2ef1ff64c66b641cf- SHA-1: b37df06dab38c08c4ad9a

Link	Applies To	File Name	File Size	Checksum
Download	Airwall ramips (100g and 100e Airwall Gateways)	HIPswitch-ramips_r2.1.4-777_package	12840142	MD5: e14c89e5b47b303ef8f609 SHA-1: c138075c7b6427fb99b2a
Download	Airwall mvebu (All 250-series Airwall Gateways)	HIPswitch-mvebu_r2.1.4-891_package	22979484	MD5: 6c2c2e9a5e2ddb03dc9da SHA-1: 58bdeabc3c404676bc43d
Download	Airwall x86_64 (100rc, all 300-series, 400-series, and 500-series Airwall Gateways)	HIPswitch-x86_64_r2.1.4-1182_package	18311139	MD5: ec430c60e0e7f36e19f2a6 SHA-1: 3a67079f798d1b6b3f682
Download	Airwall x86_64 OVA (ESXi)	HIPswitch-x86_64_r2.1.4-1182-combined-ext4.ova	20084736	MD5: 3cd09a8a879c6ed734b78 SHA-1: 64298c83d9f9e530df9aa1
Download	Airwall x86_64 VHD (Hyper-V)	HIPswitch-x86_64_r2.1.4-1182-combined-ext4.vhd	139461120	MD5: 44febc8e50d44ea6362e0 SHA-1: 5ef4dc6ffa08f0c0153d98

Software

Link	Applies To	File Name	File Size	Checksum
Download	Airwall Agent (Windows)	HIPclient64_2.1.4.457_18261045_Installer.exe	18261045	MD5: e4b21604879c2dd7acc67 SHA-1: 220f6f9f99514619b1913
Download	Airwall Server (Windows)	HIPserver64_2.1.4.631_182655045_Installer.exe	182655045	MD5: 3aa38ed65aa812fd5f865a SHA-1: b8a495810624a5afcbdb3
Download	Airwall Agent (OSX, macOS)	HIPclient_2.1.4.1046.pkg	1046	MD5: a9ac9996a9623bd79d8b5 SHA-1: 517b031d2f96db3063faaff
Download	Airwall Server (Linux/Ubuntu)	hipserver_2.1.4-858_amd64.deb	858	MD5: 98691f27c5b98d4ad1994 SHA-1: bebfe567c10c992198182
Download	Airwall Server (Linux/CentOS)	hipserver-2.1.4-655.el7.x86_64.rpm	655	MD5: 9f3d8dd6f36e8ef92d9a78 SHA-1: 4542be30ae588a11d2a25

2.1.3 firmware and software

Please follow the links below to download version 2.1.3 firmware:

Conductor firmware:

- [Conductor \(All platforms\)](#)

Airwall firmware:

- [HIPswitch ramips \(100g and 100e HIPswitches\)](#)

- Airwall Gateway Cns3xxx (All 200-series Airwall Gateways)
 - Important:** The HIPswitch 200 Series is not supported on software versions later than 2.1.2. Please see product bulletin End of Life for HIPswitch 200 Series for more information.
- Airwall mvebu (All 250-series Airwall Gateways)
- HIPswitch x86_64 (100rc, all 300-series, 400-series, and 500-series HIPswitches)

Software:

- Airwall Agent (Windows)
- Airwall Server (Windows)
- Airwall Agent (MacOS)
- Airwall Server (Linux/Ubuntu)
- Airwall Server (Linux/CentOS)



Note: The iOSAirwall Agent is available in the App Store.

Virtual Images:

- HIPswitch x86_64 OVA (ESXi)
- HIPswitch x86_64 VHD (Hyper-V)

2.1.2 firmware and software

Please follow the links below to download version 2.1.2 firmware:

Conductor firmware:

- Conductor (All platforms)

HIPswitch firmware:

- HIPswitch ramips (100g and 100e Airwall Gateways)
- HIPswitch Cns3xxx (All 200-series Airwall Gateways)
- HIPswitch_mvebu (All 250-series Airwall Gateways)
- HIPswitch_x86_64 (100rc, all 300-series and 400-series Airwall Gateways)

Software:

- Airwall Agent (Windows)
- Airwall Server (Windows)
- Airwall Agent (MacOS)

Virtual Images:

- HIPswitch x86_64 OVA (ESXi)
- HIPswitch x86_64 VHD (Hyper-V)

Hotfixes

Please follow the links below to download the hotfix for your platform. For hotfixes before 2.1.x, see [pre-Airwall Hotfixes](#).

2.2.12 Hotfixes

Download	Applies to:	Date	Behavior
2.2.12 Conductor Hotfix HF-15748	2.2.12 Conductors	May 28, 2021	See Release Notes 2.2.12 Hotfix – Conductor HF-15748 on page 489.

2.2.11 Hotfixes

Download	Applies to:	Date	Behavior
2.2.11 Conductor Hotfix HF-1	2.2.11 Conductors	Apr 13, 2021	See Release Notes 2.2.11 Hotfix – Conductor HF-1 on page 500.
2.2.11 Airwall Gateway Hotfix HF-2	2.2.11 Airwall Gateways	Mar 30, 2021	See Release Notes 2.2.11 Hotfix – Airwall Gateway HF-2 on page 501.
2.2.11 Airwall Gateway Hotfix HF-1	2.2.11 Airwall Gateways	Mar 17, 2021	See Release Notes 2.2.11 Hotfix – Airwall Gateway HF-1 on page 501.

2.2.10 Hotfixes

Download	Applies to:	Date	Behavior
2.2.10 Airwall Gateway Hotfix HF-1	2.2.10 Airwall Gateways	Dec 16, 2020	See Release Notes 2.2.10 Hotfix – Airwall Gateway HF-1 on page 513.
2.2.10 Conductor Hotfix HF-1	2.2.10 Conductor	Dec 16, 2020	See Release Notes 2.2.10 Hotfix – Conductor HF-1 on page 514

2.2.8 Hotfixes

Download	Applies to:	Date	Behavior	Notes
Conductor HF-5 Includes Conductor HF-1 through HF-4	2.2.8	Dec 18, 2020	Short password reset timeout for new users.	See Release Notes 2.2.8 Hotfix – Conductor HF-5 on page 530.
TPM keystore Airwall Gateway Hotfix-14558	2.2.8	Nov 18, 2020	Airwall Gateways using a TPM keystore fail to upgrade to 2.2.10.	For v2.2.8 Airwall Gateways that use a TPM keystore, install this hotfix before upgrading to v2.2.10.
Airwall Gateway Hotfix HF-3 Includes HF-1 and 2	2.2.8 Airwall Gateways	Oct 19, 2020	See Release Notes 2.2.8 Hotfix – Airwall Gateway HF-3 on page 533	Install the hotfix to resolve issues fixed in this hotfix, or in retired Airwall Gateway hotfixes HF-2 or HF-1.

Download	Applies to:	Date	Behavior	Notes
2.2.8 Conductor Hotfix HF-4 Includes HF-1, 2, and 3	2.2.8 Conductor	Oct 19, 2020	Release Notes 2.2.8 Hotfix – Conductor HF-4 on page 534	Install the hotfix to resolve issues fixed in this hotfix, or in retired Conductor hotfixes HF-3, HF-2, or HF-1.
2.2.8 Airwall Gateway Hotfix-13955	2.2.8 Airwall Gateways	Aug 4, 2020	See Release Notes 2.2.8 Hotfix – Airwall Gateway Hotfix-13955 on page 537 .	Install this hotfix before upgrading Airwall Gateways to 2.2.8.
<i>Retired 2.2.8 Hotfixes</i>				
Airwall Gateway Hotfix HF-2 (Retired)	2.2.8 Airwall Gateway	Sep 15, 2020	See Release Notes 2.2.8 Hotfix – Airwall Gateway HF-2 (Retired) on page 641 .	Retired
Conductor Hotfix HF-3 (Retired)	2.2.8 Conductor	Sep 3, 2020	See Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired) on page 643	Retired
Airwall Gateway Hotfix HF-1 (Retired)	2.2.8 Airwall Gateways	Sep 3, 2020	See Release Notes 2.2.8 Hotfix – Airwall Gateway HF-1 (Retired) on page 642 .	Retired
2.2.8 Conductor Hotfix HF-2 (Retired)	2.2.8 Conductor	Aug 19, 2020	See Release Notes 2.2.8 Hotfix – Conductor HF-2 (Retired) on page 645	Retired
2.2.8 Conductor Hotfix HF-1 (Retired)	2.2.8 Conductor	July 30, 2020	See Release Notes 2.2.8 Hotfix – Conductor HF-1 (Retired) on page 646 .	Retired

2.1.x Series Hotfixes

Download	Applies to:	Date	Behavior	Resolution
Hotfix 8551	HIPswitch 250 Series running version 2.1.3	August 23, 2018	HIPswitch repeatedly connects and disconnects. See Product Bulletin 201808B-001 for more information.	Apply Hotfix 8551 to resolve the issue.

Download	Applies to:	Date	Behavior	Resolution
Hotfix 8543	HIPswitch 100 Series running version 2.1.3	August 23, 2018	HIPswitch repeatedly connects and disconnects. See Product Bulletin 201808B-001 for more information.	Apply Hotfix 8543 to resolve the issue.
Hotfix 7414	2.1.2 virtual HIPswitches running in VMware ESXi	March 15, 2018	VMware reports 100% CPU usage when running a 2.1.2 virtual HIPswitch	Apply Hotfix 7414 to resolve the issue.

Release Notes

Release notes track incremental improvements and major releases for the Airwall solution, software applications, and our physical, virtual, and cloud platforms. For older Release Notes, see [pre-2.2.3 help](#).

Latest Release Notes (v3.0)

Release Notes v3.0.0

Release Date: Nov 2, 2021

Important Notes

- **Update all v2.1.x Airwall Edge Services** – It is recommended that you update all v2.1.x and earlier Airwall Edge Services with v2.2.x or later before installing v3.0. With this release, any Airwall Edge Services running v2.1.x firmware show an error in the Conductor. For more information, see [Update v2.1.x Airwall Edge Services for the v3.0 Conductor](#) on page 418.
- **If you are updating a virtual Conductor to v3.0** – You may need to expand the disk size for the virtual machine to 1GB. For instructions, see your virtual machine documentation, or the suggested VMware and Hyper-V instructions at [Expand the Disk Size for a virtual Airwall Gateway](#) on page 265.

End of Life/End of Support Bulletins

- **2.1.x End of Life** – See [Software support end of life for versions 2.1.x and earlier](#) on page 422. For update instructions, see [Update v2.1.x Airwall Edge Services for the v3.0 Conductor](#) on page 418.
- **Ubuntu16 and Centos7 End of Support** – See [Linux OS End of Support](#) on page 423

Update Considerations

You may want to update to this version to use the following features:.

- [Backhaul Bypass](#) on page 333
- [Import people using a CSV file](#) on page 51
- [Customize Permissions for System and Network Administrators](#) on page 46
- [Customize the Conductor Login page](#) on page 41
- [Customize Conductor emails](#) on page 42
- [Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers](#) on page 82
- Airwall Invitation improvements – [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71
- [Linux Airwall Server Airshell commands](#) on page 309
- [Manage Failover between Underlay Port Groups](#) on page 326

- [Run Network Activity Reports](#) on page 101

Downloads

For firmware and software downloads for this version, see [3.0 firmware and software](#) on page 433.

What's New in 3.0

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and administration of an Airwall secure network.

Add Trust Policy using Drag-and-drop

You can now add and remove trust between devices on an overlay visually, or through context menus on a graph. Changes to trust on the graph are reflected on the **Devices** tab.

Learn more – [Add and remove device trust](#) on page 360

Backhaul Bypass

You can designate an Airwall Gateway as a bypass egress and then point other Airwall Gateways at it so they can reach bypass destinations through the designated bypass egress Airwall Gateway.

Learn more – [Backhaul Bypass](#) on page 333

Bulk Editing of People and People Groups

You can add many local users to the Conductor at one time by importing them in bulk. You export a .csv file as a template or with current users, and then import to add people to the Conductor in one step.

Learn more –

- [Import people using a CSV file](#) on page 51
- [Remove people in bulk](#) on page 53

Customized Permissions for System and Network Administrators

You can fine tune permissions for system and network administrators, giving you finer control over permissions on your network.

Learn more – [Customize Permissions for System and Network Administrators](#) on page 46

Streamlined Conductor View for Network Administrators

One of the custom permissions you can set for Network administrators provides them with a streamlined view that can simplify their workflow. Network administrators using the streamlined view can manage their overlays, and the devices, **Device groups**, and Airwall Edge Services in them.

Learn more – [Set a Streamlined View for a Network Administrator](#) on page 48

Reports

You can now run reports on different types of network activity on your Airwall secure network, including:

- Onboarding and offboarding of Airwall Edge Services or people
- Status of Airwall Edge Services or devices
- Conductor local or remote access

Learn more – [Run Network Activity Reports](#) on page 101

Monitors and Alerts

This version includes the following additions:

- **CPU Frequency** – The Airwall health data monitors can now monitor CPU frequency.
- **Details for Intrusion prevention** – Intrusion prevention alerts now indicate which devices are the source or destination of the alert where possible.

Conductor Customization

You can customize the Conductor login screen and emails sent from the Conductor for your business. Here's what you can customize:

- **Conductor login screen** – Add your company logo, and change the background colors and favicon.
- **Conductor emails** – Add your company logo and change the text color. You can also customize the subject line and add a note from the administrator when sending Airwall Invitations.

Learn more –

- [Customize the Conductor](#) on page 41
- [Customize the Conductor Login page](#) on page 41
- [Customize Conductor emails](#) on page 42

Disconnected Mode

Reduce the traffic from Airwall Agents and Servers connecting to your Conductor by setting up Disconnected mode. In Disconnected mode, Airwall Agents and Servers connect to your Conductor at intervals – between 10 minutes and 12 hours (720 minutes) – to get updates when people are not actively using the connection.

By reducing the traffic on your Conductor, Disconnected mode allows you to improve performance and scalability of your Airwall secure network. In v3.0, Disconnected mode is supported by the v3.0 Android, Linux, and macOS Airwall Agents and Servers.

Learn more –

- [Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers](#) on page 82
- [Sync an Airwall Agent or Server in Disconnected Mode](#) on page 29

Airwall Invitations

This version includes several enhancements to Airwall Invitations:

- When you're creating **People groups** with user onboarding enabled, you now have the option to send email to users when they get an activation code in the system. The email provides instructions on how to download an Airwall Agent and connect it to the Conductor.
- The email sent with Airwall Invitations has more options for customization. See **Conductor Customization** above.
- Airwall Invitations can now be used to give activation codes to existing users in addition to sending them to an email address or bulk downloading them. See the [Airwalls > New Airwall invitations](#).
- The naming schema for Airwall Invitations can now include the hostname of the connecting Airwall Edge Service.
- You can now include the hostname of the connecting Airwall Edge Service when naming devices connecting using Airwall Invitations.

Learn more – [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71

Linux Airwall Server

This version includes these additions to the Linux Airwall Server:

- **DockerHub deployment** – The Linux Airwall Server can now be deployed in a container from [DockerHub](#) using Ubuntu18 and CentOS8. For additional example Dockerfiles, contact Customer Success at support@tempered.io.
- **Supports Airshell** – The Linux Airwall Server now has the Airshell command-line utility. To start it, type `sudo airsh (root user)` or `sudo airwall -s`

- **Ping from port groups** – The ping function can now ping from the underlay or overlay port groups.
- **Firmware updates** – The Linux Airwall Server can now be updated from the Conductor.

Learn more –

- [Connect with a Linux Airwall Server](#) on page 26
- [Linux Airwall Server Airshell commands](#) on page 309

Conductor Tutorials and Help

The Conductor now contains several tutorials to help you set up and configure a new Conductor, as well as use and understand different features in the Conductor. You can also directly access Airwall help from the Conductor:

Learn more –

- [Get Started using Conductor Help and Tutorials](#) on page 118
- [Show or Hide Conductor Setup progress](#) on page 30

Licensing Updates

In v3.0, the following licenses have been changed:

- The Airwall Gateway 100V is no longer available
- You no longer need a separate license for port mirroring

Manage failover between underlay port groups

The Link Manager that Conductor uses to manage port failover groups has been improved. The following has been updated:

- You can now set port group link auto-repair globally per Airwall Gateway.
- You can now manage underlay links independently by traffic type.
- When you set up link failover groups, you can now require all pings to be successful if multiple ping destinations are assigned.

Learn more – [Manage Failover between Underlay Port Groups](#) on page 326

API Updates

The following updates and improvements have been made to the API:

- **Pagination** is turned on by default in 3.0 for all index endpoints, which may affect existing scripts. Enabling pagination helps scale Conductor capacity. If you need to preserve existing behavior, add a query parameter for `pagination=false` to any index API endpoints you are using.
- The API for **Airwall Invitations** now includes new invitation methods: email invites, download multiple activation codes, apply an invite to an existing person, or download a reusable invitation. The documentation has also been updated.
- **People reference** now includes `person_group_ids` and `overlay_network_ids`.
- **Person groups reference** now includes user onboarding configuration information.

Terraform Deployment Support

This version contains Terraform deployment support for Conductors, Airwall Gateways, and Linux Airwall Servers for all supported Cloud Providers. For example plans, please contact Customer Success at support@tempered.io.

New and Improved Conductor Features

Dashboard

The Dashboard now includes a **Provisioning** tab where you can see and manage all provisioning requests.

General

There is now infinite scrolling for lists on most pages, and streamlined inline editing, including direct editing of names and tags at the top on most pages.

Devices page

This page has been simplified, and provides more details on device conflicts to help you troubleshoot.

People page

Administrators can now view the Airwalls owned by a person from the person details page.

Settings

The Conductor Settings page has been streamlined and reorganized to make it easier to find the settings you want.

New Airwall Agent user authentication settings

New settings allow you to automate assigning an Airwall Agent owner: **Require owner for Airwall Agent authorization** and **Auto-assign Airwall agent owner on login**.

Replacing Airwalls

You now have the option to revoke, or both revoke and delete, a source Airwall Edge Service after replacing. Replaced Airwall Edge Services that are not deleted are named "<old name (Replaced by UID of replacement)>" to make them easier to find.

Diagnostic Tools on the Standby Conductor

You can now use diagnostic tools on a Standby Conductor.

Better CA certificate replacement and removal handling

When you replace your CA certificates, any Airwall Gateways with custom certs installed now check their cert against the new CA. If they cannot be verified, the cert is removed so the Airwall Gateway does not lose access to the Conductor. If the CA is removed entirely, all customer certs are also removed.

Learn more –

- [The Conductor Dashboard](#) on page 32
- [Configure Authentication Options](#) on page 203

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- [Expand the Disk Size for a virtual Airwall Gateway](#) on page 265
- [Airwall Gateway 75 Installation Guide \(PDF\)](#)

Updated –

- [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71
- [Configure Port Groups with Airshell](#) on page 312
- [Set up Conductor high availability](#) on page 231
- [Manage devices dynamically with Smart Device Groups](#) on page 87
- [Configure a Conductor IP, Friendly URL, or Port](#) on page 198
- [Understand People Roles and Permissions](#) on page 49
- [Configure Conductor Remote Logging](#) on page 236
- [Enable DNS lookup for bypass destinations](#) on page 336
- [Monitor Activity and Connections](#) on page 100
- [Integrate Third-party Authentication with OpenID Connect](#) on page 208
- [Airwall Gateway Airshell Console Commands - airsh](#) - New conf model command

Fixes

ID	Applies to	Description
DEV-16491	Cellular Airwall Gateways	Fixed an issue where underlay interface MTU was not considered in tunnel overlay MTU, and another where the path MTU didn't work correctly across local bypass configurations. Known issue – The path MTU doesn't work across backhaul bypass. Make sure any backhaul bypass egress Airwall Gateways have a full 1500 byte standard Ethernet MTU (that is, do not use a cell modem).
DEV-16233	Airwall Gateways	Fixed an issue where Ping <ip or hostname> (in Airwall Diagnostics) returned false negatives for hostnames longer than 46 bytes.
DEV-16102	Airshell, Airwall Gateways	The Airshell firmware-fallback command is now functional on Advantech (Airwall AV-3200 series).
DEV-15942	Airwall Gateways	Fixed a DNS resolver issue that could cause long delays for Airwall Gateways trying to reconnect to the Conductor when configured with a hostname.
DEV-15938	Airshell	The 'activate' command in Airshell now takes the activation code as an optional argument. For example, activate 75820b33fa5a.
DEV-15860	Hardware Conductor	Fixed an issue where the Conductor-500 LCD panel would display "Conductor unreachable".
DEV-15835	Conductor	Fixed an issue where the Traffic stats monitor alerts indicated traffic in kB/s when the correct value is Kb/s (kilobits per second).
DEV-15784	Diagnostic mode	Fixed an issue where bridging all overlay interfaces was causing problems when an Airwall Gateway was in Diag mode.
DEV-15762	Conductor	Fixed an issue where readonly users appeared to be able to edit some tag-related event actions.
DEV-15761	Conductor	Fixed an issue where readonly users appeared to be able to edit some person group user onboarding settings.
DEV-15760	Conductor	Intrusion prevention controls are now disabled unless the user has edit permission for the Airwall Edge Service.

ID	Applies to	Description
DEV-15759	Conductor	Fixed an issue where readonly users appeared to be able to create Airwall Invitations with a template.
DEV-15757	Conductor	Fixed an issue where readonly users appeared to be able to edit tags.
DEV-15736	Airwall Gateways	Fixed an issue where the Ping Peers diagnostic feature didn't support multiple peers with the same underlay IP address.
DEV-15707	Conductor	Fixed an issue where users could not remove all relays from an overlay-managed relay rule.
DEV-15679	Conductor	Your previous login selection is now saved regardless of provider (local, LDAP, or OpenID connect).
DEV-15653	Conductor	Instructions for setting up OpenID Connect on HA standby Conductors are now clearer.
DEV-15534	Cloud Airwall Gateways	Fixed an issue where detecting the underlay NAT IP of a cloud 300v Airwall Gateway wasn't being sent to peer Airwall Gateways
DEV-15525	Conductor	Fixed an issue during a device import where you could select Next even though there was an error.
DEV-15420	Conductor	Fixed an issue where you could enable passive device discovery before selecting an Overlay port group.
DEV-15393	Linux Airwall Servers	Fixed the invalid log level error message when starting up a Linux Airwall Server.
DEV-15203	Airwall Gateways	Fixed an issue that could cause passive device detection to ignore devices when traffic is seen immediately after reboot.
DEV-14908	Conductor	Display a warning when there is a mismatch in authentication providers for an Airwall Agent owner and the user auth allowed in the Conductor that would prevent a user from authenticating a remote session.
DEV-14608	Airwall Gateways	Fixed an issue that could prevent initialization of port groups with VLAN interfaces if the parent port was removed from another port group.
DEV-14471	Diagnostic mode	Port group numbers are no longer incremented by 2 in diag mode.
DEV-14318	Conductor, Linux Airwall Servers	Fixed an issue where the Linux Airwall Server wouldn't always get policy updates until it was rebooted.
DEV-13587	Conductor	Clarified language in the Add / Remove tag monitor action.
DEV-11607	Airwall Gateways	Fixed an issue in the health data capture for Airwall Gateways that showed all overlay ports as having no link.
DEV-11524	Android Airwall Agents	Fixed an issue where Android was reporting incorrect IPs for interfaces on its Ports tab in the Conductor.

Known Issues

ID	Applies to	Description
DEV-16503	macOS Airwall Agents	<p>Deleting a profile does not immediately delete the associated private key.</p> <p>Workaround – Switch to a different profile before creating a profile after deleting one.</p>
DEV-16397	Conductor	<p>If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to Settings > Diagnostics and select Restart metadata cache to update the LSI prefix.</p>
DEV-16322	Conductor	<p>If a person is in more than one person group that has access windows set for the group, they can only authenticate for a remote session during times that are inside all of the access windows for those person groups.</p>
DEV-16068	Amazon Web Services Conductor	<p>To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.</p>
DEV-16059	Airwall Gateways	<p>When HA-pairing two Airwall Gateways that don't have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.</p>
DEV-15982	Conductor	<p>Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.</p>
DEV-15887	Airwall Gateways	<p>You cannot currently add VLAN interfaces to the Ruggedcom platform.</p>
DEV-15808	Google Cloud Airwall Gateways	<p>Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor.</p> <p>Workaround – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.</p>
DEV-15791	Airwall Gateways	<p>On the Airwall Gateway 100, Port 2 might be inactive after a factory-reset.</p> <p>Workaround – After a factory reset, manually reboot the Airwall Gateway 100.</p>

ID	Applies to	Description
DEV-15787	macOS Airwall Agents	<p>If a person who already has a profile makes a Request to Connect from the Remote Access User portal on the same Conductor, no profile is created.</p> <p>Workaround – If the user wants a second profile, they can use an invite code or enter the Conductor information manually.</p>
DEV-15705	macOS Airwall Agents	<p>Establishing a tunnel TO a mobile Airwall Agent (iOS or Android) fails when there is no Airwall Relay involved.</p> <p>Workaround – Establish the tunnel FROM the mobile Airwall Agent.</p>
DEV-15572	Airwall Gateways	<p>If you don't specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway.</p> <p>Workaround – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See https://tempered.force.com/TemperedSupportCenter/s/article/DHCP-server-isn-t-serving-as-a-gateway.</p>
DEV-15357	macOS Airwall Agents	<p>If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor.</p> <p>Workaround – Restart the Airwall Agent or reapply the update.</p>
DEV-15338	Linux Airwall Servers	<p>If using a recent systemd-based Linux distribution including Fedora 33 and Debian 11, disable systemd-networkd MAC address randomization of the hip1 interface.</p>

ID	Applies to	Description
DEV-15302	macOS Airwall Agents	<p>The profile for a macOS Airwall Agent does not work correctly when restored to a new computer using Time Machine.</p> <p>Workaround – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one.</p>
DEV-15219	Cellular 110g Airwall Gateways	<p>The Airwall Gateway 110g does not work on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.</p>
DEV-15031	Airwall Gateways	<p>Remote syslog over TLS doesn't work when using keys stored in TPM.</p>
DEV-14860	Conductor	<p>Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.</p>
DEV-14835	Conductor	<p>Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.</p>
DEV-14739	Airwall Gateways	<p>If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved.</p> <p>Workaround – If you need both IPv4 and IPv6, set static IP addresses for both.</p>
DEV-14736	Cellular Airwall Gateways	<p>Cellular details may display as "unavailable" on the first boot after you update an Airwall Gateway. The cellular connections are not affected.</p> <p>Workaround – Reboot the Airwall Gateway again to correctly display the cellular details.</p>
DEV-14726	Conductor	<p>If you're viewing an Android Airwall Agent Ports tab and the Airwall Agent changes how it's connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly.</p> <p>Workaround – Refresh the page.</p>
DEV-14715	macOS Airwall Agents	<p>Big Sur ARM64 Macs are not supported in this release</p>
DEV-14610	Conductor	<p>After changing the Reporting traffic stats reporting time, the CPU graph does not display.</p> <p>Workaround – Refresh your browser page.</p>

ID	Applies to	Description
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work.
		Workaround – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14570	Conductor	If you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 instead of a helpful error message.
DEV-14551	Conductor	The Android Airwall Agent lets you press the Edit Settings button on the Ports page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14249	iOS Airwall Agents	Check Secure Tunnels Tunnel Status may show as unavailable on iOS.
		Workaround – You can determine tunnel status by checking packets sent or received.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14045	Android and iOS Airwall Agents	iOS does not currently support overlay ping.
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay.
		Workaround – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway Local Devices tab.

ID	Applies to	Description
DEV-13640	Conductor	Airwall Relay diagnostics don't work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. Workaround – Download firmware from the active Conductor.
DEV-13620	Conductor	In Airwall > Ports > Failover settings , the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (Airwall > Ports > Failover settings) does not apply the settings to any port groups. You must also assign the failover group to port groups on the Ports page.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. Workaround – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. Workaround – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. Workaround – Change the Conductor system time to browser time: In Conductor Settings , under System time , select Edit Settings , select Set browser time , and then select Update Settings .
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." Workaround – Reboot and the details return.
DEV-13194	Conductor	Check Connectivity > Ping Local Devices for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. Workaround – Use one of the latest versions of Chrome, Firefox, Safari or Edge.

ID	Applies to	Description
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. Workaround – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.

Release Notes v3.0.0

Release Date: Nov 2, 2021

Important Notes

- Update all v2.1.x Airwall Edge Services** – It is recommended that you update all v2.1.x and earlier Airwall Edge Services with v2.2.x or later before installing v3.0. With this release, any Airwall Edge Services running v2.1.x firmware show an error in the Conductor. For more information, see [Update v2.1.x Airwall Edge Services for the v3.0 Conductor](#) on page 418.
- If you are updating a virtual Conductor to v3.0** – You may need to expand the disk size for the virtual machine to 1GB. For instructions, see your virtual machine documentation, or the suggested VMware and Hyper-V instructions at [Expand the Disk Size for a virtual Airwall Gateway](#) on page 265.

End of Life/End of Support Bulletins

- 2.1.x End of Life** – See [Software support end of life for versions 2.1.x and earlier](#) on page 422. For update instructions, see [Update v2.1.x Airwall Edge Services for the v3.0 Conductor](#) on page 418.
- Ubuntu16 and Centos7 End of Support** – See [Linux OS End of Support](#) on page 423

Update Considerations

You may want to update to this version to use the following features:..

- [Backhaul Bypass](#) on page 333
- [Import people using a CSV file](#) on page 51
- [Customize Permissions for System and Network Administrators](#) on page 46
- [Customize the Conductor Login page](#) on page 41
- [Customize Conductor emails](#) on page 42
- [Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers](#) on page 82
- [Airwall Invitation improvements – Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71
- [Linux Airwall Server Airshell commands](#) on page 309
- [Manage Failover between Underlay Port Groups](#) on page 326
- [Run Network Activity Reports](#) on page 101

Downloads

For firmware and software downloads for this version, see [3.0 firmware and software](#) on page 433.

What's New in 3.0

This version of the Airwall Solution includes several usability and functionality improvements that can simplify and streamline the setup and administration of an Airwall secure network.

Add Trust Policy using Drag-and-drop

You can now add and remove trust between devices on an overlay visually, or through context menus on a graph. Changes to trust on the graph are reflected on the **Devices** tab.

Learn more – [Add and remove device trust](#) on page 360

Backhaul Bypass

You can designate an Airwall Gateway as a bypass egress and then point other Airwall Gateways at it so they can reach bypass destinations through the designated bypass egress Airwall Gateway.

Learn more – [Backhaul Bypass](#) on page 333

Bulk Editing of People and People Groups

You can add many local users to the Conductor at one time by importing them in bulk. You export a .csv file as a template or with current users, and then import to add people to the Conductor in one step.

Learn more –

- [Import people using a CSV file](#) on page 51
- [Remove people in bulk](#) on page 53

Customized Permissions for System and Network Administrators

You can fine tune permissions for system and network administrators, giving you finer control over permissions on your network.

Learn more – [Customize Permissions for System and Network Administrators](#) on page 46

Streamlined Conductor View for Network Administrators

One of the custom permissions you can set for Network administrators provides them with a streamlined view that can simplify their workflow. Network administrators using the streamlined view can manage their overlays, and the devices, **Device groups**, and Airwall Edge Services in them.

Learn more – [Set a Streamlined View for a Network Administrator](#) on page 48

Reports

You can now run reports on different types of network activity on your Airwall secure network, including:

- Onboarding and offboarding of Airwall Edge Services or people
- Status of Airwall Edge Services or devices
- Conductor local or remote access

Learn more – [Run Network Activity Reports](#) on page 101

Monitors and Alerts

This version includes the following additions:

- **CPU Frequency** – The Airwall health data monitors can now monitor CPU frequency.
- **Details for Intrusion prevention** – Intrusion prevention alerts now indicate which devices are the source or destination of the alert where possible.

Conductor Customization

You can customize the Conductor login screen and emails sent from the Conductor for your business. Here's what you can customize:

- **Conductor login screen** – Add your company logo, and change the background colors and favicon.
- **Conductor emails** – Add your company logo and change the text color. You can also customize the subject line and add a note from the administrator when sending Airwall Invitations.

Learn more –

- [Customize the Conductor](#) on page 41
- [Customize the Conductor Login page](#) on page 41
- [Customize Conductor emails](#) on page 42

Disconnected Mode

Reduce the traffic from Airwall Agents and Servers connecting to your Conductor by setting up Disconnected mode. In Disconnected mode, Airwall Agents and Servers connect to your Conductor at intervals – between 10 minutes and 12 hours (720 minutes) – to get updates when people are not actively using the connection.

By reducing the traffic on your Conductor, Disconnected mode allows you to improve performance and scalability of your Airwall secure network. In v3.0, Disconnected mode is supported by the v3.0 Android, Linux, and macOS Airwall Agents and Servers.

Learn more –

- [Disconnected Mode – Reduce Conductor traffic from Airwall Agents and Servers](#) on page 82
- [Sync an Airwall Agent or Server in Disconnected Mode](#) on page 29

Airwall Invitations

This version includes several enhancements to Airwall Invitations:

- When you're creating **People groups** with user onboarding enabled, you now have the option to send email to users when they get an activation code in the system. The email provides instructions on how to download an Airwall Agent and connect it to the Conductor.
- The email sent with Airwall Invitations has more options for customization. See **Conductor Customization** above.
- Airwall Invitations can now be used to give activation codes to existing users in addition to sending them to an email address or bulk downloading them. See the [Airwalls > New Airwall invitations](#).
- The naming schema for Airwall Invitations can now include the hostname of the connecting Airwall Edge Service.
- You can now include the hostname of the connecting Airwall Edge Service when naming devices connecting using Airwall Invitations.

Learn more – [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71

Linux Airwall Server

This version includes these additions to the Linux Airwall Server:

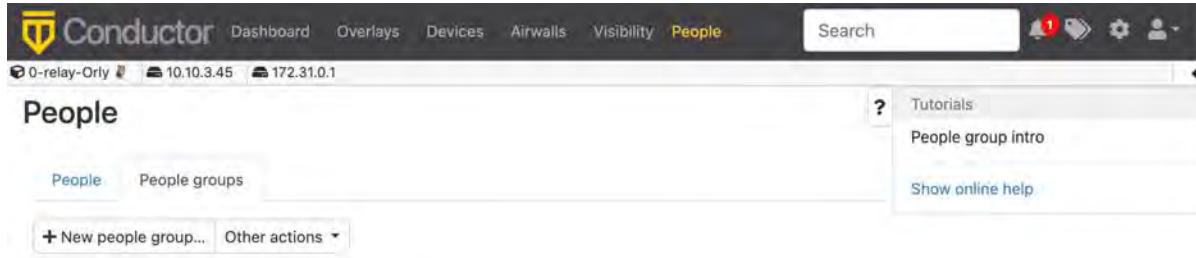
- **DockerHub deployment** – The Linux Airwall Server can now be deployed in a container from [DockerHub](#) using Ubuntu18 and CentOS8. For additional example Dockerfiles, contact Customer Success at support@tempered.io.
- **Supports Airshell** – The Linux Airwall Server now has the Airshell command-line utility. To start it, type `sudo airsh` (root user) or `sudo airwall -s`
- **Ping from port groups** – The ping function can now ping from the underlay or overlay port groups.
- **Firmware updates** – The Linux Airwall Server can now be updated from the Conductor.

Learn more –

- [Connect with a Linux Airwall Server](#) on page 26
- [Linux Airwall Server Airshell commands](#) on page 309

Conductor Tutorials and Help

The Conductor now contains several tutorials to help you set up and configure a new Conductor, as well as use and understand different features in the Conductor. You can also directly access Airwall help from the Conductor:



Learn more –

- [Get Started using Conductor Help and Tutorials](#) on page 118
- [Show or Hide Conductor Setup progress](#) on page 30

Licensing Updates

In v3.0, the following licenses have been changed:

- The Airwall Gateway 100V is no longer available
- You no longer need a separate license for port mirroring

Manage failover between underlay port groups

The Link Manager that Conductor uses to manage port failover groups has been improved. The following has been updated:

- You can now set port group link auto-repair globally per Airwall Gateway.
- You can now manage underlay links independently by traffic type.
- When you set up link failover groups, you can now require all pings to be successful if multiple ping destinations are assigned.

Learn more – [Manage Failover between Underlay Port Groups](#) on page 326

API Updates

The following updates and improvements have been made to the API:

- **Pagination** is turned on by default in 3.0 for all index endpoints, which may affect existing scripts. Enabling pagination helps scale Conductor capacity. If you need to preserve existing behavior, add a query parameter for `pagination=false` to any index API endpoints you are using.
- The API for **Airwall Invitations** now includes new invitation methods: email invites, download multiple activation codes, apply an invite to an existing person, or download a reusable invitation. The documentation has also been updated.
- **People reference** now includes `person_group_ids` and `overlay_network_ids`.
- **Person groups reference** now includes user onboarding configuration information.

Terraform Deployment Support

This version contains Terraform deployment support for Conductors, Airwall Gateways, and Linux Airwall Servers for all supported Cloud Providers. For example plans, please contact Customer Success at support@tempered.io.

New and Improved Conductor Features

Dashboard

The Dashboard now includes a **Provisioning** tab where you can see and manage all provisioning requests.

General

There is now infinite scrolling for lists on most pages, and streamlined inline editing, including direct editing of names and tags at the top on most pages.

Devices page

This page has been simplified, and provides more details on device conflicts to help you troubleshoot.

People page

Administrators can now view the Airwalls owned by a person from the person details page.

Settings

The Conductor Settings page has been streamlined and reorganized to make it easier to find the settings you want.

New Airwall Agent user authentication settings

New settings allow you to automate assigning an Airwall Agent owner: **Require owner for Airwall Agent authorization** and **Auto-assign Airwall agent owner on login**.

Replacing Airwalls

You now have the option to revoke, or both revoke and delete, a source Airwall Edge Service after replacing. Replaced Airwall Edge Services that are not deleted are named "<old name (Replaced by UID of replacement)>" to make them easier to find.

Diagnostic Tools on the Standby Conductor

You can now use diagnostic tools on a Standby Conductor.

Better CA certificate replacement and removal handling

When you replace your CA certificates, any Airwall Gateways with custom certs installed now check their cert against the new CA. If they cannot be verified, the cert is removed so the Airwall Gateway does not lose access to the Conductor. If the CA is removed entirely, all customer certs are also removed.

Learn more –

- [The Conductor Dashboard](#) on page 32
- [Configure Authentication Options](#) on page 203

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- [Expand the Disk Size for a virtual Airwall Gateway](#) on page 265
- [Airwall Gateway 75 Installation Guide \(PDF\)](#)

Updated –

- [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71
- [Configure Port Groups with Airshell](#) on page 312
- [Set up Conductor high availability](#) on page 231
- [Manage devices dynamically with Smart Device Groups](#) on page 87

- [Configure a Conductor IP, Friendly URL, or Port](#) on page 198
- [Understand People Roles and Permissions](#) on page 49
- [Configure Conductor Remote Logging](#) on page 236
- [Enable DNS lookup for bypass destinations](#) on page 336
- [Monitor Activity and Connections](#) on page 100
- [Integrate Third-party Authentication with OpenID Connect](#) on page 208
- [Airwall Gateway Airshell Console Commands - airsh](#) - New conf model command

Fixes

ID	Applies to	Description
DEV-16491	Cellular Airwall Gateways	Fixed an issue where underlay interface MTU was not considered in tunnel overlay MTU, and another where the path MTU didn't work correctly across local bypass configurations. Known issue – The path MTU doesn't work across backhaul bypass. Make sure any backhaul bypass egress Airwall Gateways have a full 1500 byte standard Ethernet MTU (that is, do not use a cell modem).
DEV-16233	Airwall Gateways	Fixed an issue where Ping <ip or hostname> (in Airwall Diagnostics) returned false negatives for hostnames longer than 46 bytes.
DEV-16102	Airshell, Airwall Gateways	The Airshell firmware-fallback command is now functional on Advantech (Airwall AV-3200 series).
DEV-15942	Airwall Gateways	Fixed a DNS resolver issue that could cause long delays for Airwall Gateways trying to reconnect to the Conductor when configured with a hostname.
DEV-15938	Airshell	The 'activate' command in Airshell now takes the activation code as an optional argument. For example, activate 75820b33fa5a.
DEV-15860	Hardware Conductor	Fixed an issue where the Conductor-500 LCD panel would display "Conductor unreachable".
DEV-15835	Conductor	Fixed an issue where the Traffic stats monitor alerts indicated traffic in kB/s when the correct value is Kb/s (kilobits per second).
DEV-15784	Diagnostic mode	Fixed an issue where bridging all overlay interfaces was causing problems when an Airwall Gateway was in Diag mode.
DEV-15762	Conductor	Fixed an issue where readonly users appeared to be able to edit some tag-related event actions.
DEV-15761	Conductor	Fixed an issue where readonly users appeared to be able to edit some person group user onboarding settings.
DEV-15760	Conductor	Intrusion prevention controls are now disabled unless the user has edit permission for the Airwall Edge Service.
DEV-15759	Conductor	Fixed an issue where readonly users appeared to be able to create Airwall Invitations with a template.
DEV-15757	Conductor	Fixed an issue where readonly users appeared to be able to edit tags.

ID	Applies to	Description
DEV-15736	Airwall Gateways	Fixed an issue where the Ping Peers diagnostic feature didn't support multiple peers with the same underlay IP address.
DEV-15707	Conductor	Fixed an issue where users could not remove all relays from an overlay-managed relay rule.
DEV-15679	Conductor	Your previous login selection is now saved regardless of provider (local, LDAP, or OpenID connect).
DEV-15653	Conductor	Instructions for setting up OpenID Connect on HA standby Conductors are now clearer.
DEV-15534	Cloud Airwall Gateways	Fixed an issue where detecting the underlay NAT IP of a cloud 300v Airwall Gateway wasn't being sent to peer Airwall Gateways
DEV-15525	Conductor	Fixed an issue during a device import where you could select Next even though there was an error.
DEV-15420	Conductor	Fixed an issue where you could enable passive device discovery before selecting an Overlay port group.
DEV-15393	Linux Airwall Servers	Fixed the invalid log level error message when starting up a Linux Airwall Server.
DEV-15203	Airwall Gateways	Fixed an issue that could cause passive device detection to ignore devices when traffic is seen immediately after reboot.
DEV-14908	Conductor	Display a warning when there is a mismatch in authentication providers for an Airwall Agent owner and the user auth allowed in the Conductor that would prevent a user from authenticating a remote session.
DEV-14608	Airwall Gateways	Fixed an issue that could prevent initialization of port groups with VLAN interfaces if the parent port was removed from another port group.
DEV-14471	Diagnostic mode	Port group numbers are no longer incremented by 2 in diag mode.
DEV-14318	Conductor, Linux Airwall Servers	Fixed an issue where the Linux Airwall Server wouldn't always get policy updates until it was rebooted.
DEV-13587	Conductor	Clarified language in the Add / Remove tag monitor action.
DEV-11607	Airwall Gateways	Fixed an issue in the health data capture for Airwall Gateways that showed all overlay ports as having no link.
DEV-11524	Android Airwall Agents	Fixed an issue where Android was reporting incorrect IPs for interfaces on its Ports tab in the Conductor.

Known Issues

ID	Applies to	Description
DEV-16503	macOS Airwall Agents	<p>Deleting a profile does not immediately delete the associated private key.</p> <p>Workaround – Switch to a different profile before creating a profile after deleting one.</p>
DEV-16397	Conductor	<p>If you change the LSI prefix and have port mirroring configured, you need to either reboot the Conductor, or go to Settings > Diagnostics and select Restart metadata cache to update the LSI prefix.</p>
DEV-16322	Conductor	<p>If a person is in more than one person group that has access windows set for the group, they can only authenticate for a remote session during times that are inside all of the access windows for those person groups.</p>
DEV-16068	Amazon Web Services Conductor	<p>To enable enhanced networking for a cloud Amazon Web Services Airwall Gateway or Conductor, use the custom images instead of the marketplace image.</p>
DEV-16059	Airwall Gateways	<p>When HA-pairing two Airwall Gateways that don't have the HA link plugged in correctly, the Conductor displays no actionable error message and the HA setup never completes.</p>
DEV-15982	Conductor	<p>Traffic stats reporting graphs generally show a smooth curve between data points. However, over time the graph can show up with sharper angles. The data is still correct, but this is a known issue with the graphing library used by the Conductor.</p>
DEV-15887	Airwall Gateways	<p>You cannot currently add VLAN interfaces to the Ruggedcom platform.</p>
DEV-15808	Google Cloud Airwall Gateways	<p>Google Cloud Airwall Gateways with the same VM name have the same device serial number, which can result in a failure when you make a license request in the Conductor.</p> <p>Workaround – In Google Cloud, use unique deployment names (VM names) for Airwall Gateways.</p>
DEV-15791	Airwall Gateways	<p>On the Airwall Gateway 100, Port 2 might be inactive after a factory-reset.</p> <p>Workaround – After a factory reset, manually reboot the Airwall Gateway 100.</p>

ID	Applies to	Description
DEV-15787	macOS Airwall Agents	<p>If a person who already has a profile makes a Request to Connect from the Remote Access User portal on the same Conductor, no profile is created.</p> <p>Workaround – If the user wants a second profile, they can use an invite code or enter the Conductor information manually.</p>
DEV-15705	macOS Airwall Agents	<p>Establishing a tunnel TO a mobile Airwall Agent (iOS or Android) fails when there is no Airwall Relay involved.</p> <p>Workaround – Establish the tunnel FROM the mobile Airwall Agent.</p>
DEV-15572	Airwall Gateways	<p>If you don't specify a gateway in the DHCP server configuration, the DHCP client cannot configure a default gateway.</p> <p>Workaround – Unless you want to configure a single isolated subnet, always specify a gateway. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway, and used in conjunction with SNAT over the overlay port group. See https://tempered.force.com/TemperedSupportCenter/s/article/DHCP-server-isn-t-serving-as-a-gateway.</p>
DEV-15357	macOS Airwall Agents	<p>If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor.</p> <p>Workaround – Restart the Airwall Agent or reapply the update.</p>
DEV-15338	Linux Airwall Servers	<p>If using a recent systemd-based Linux distribution including Fedora 33 and Debian 11, disable systemd-networkd MAC address randomization of the hip1 interface.</p>

ID	Applies to	Description
DEV-15302	macOS Airwall Agents	<p>The profile for a macOS Airwall Agent does not work correctly when restored to a new computer using Time Machine.</p> <p>Workaround – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one.</p>
DEV-15219	Cellular 110g Airwall Gateways	<p>The Airwall Gateway 110g does not work on the Bell Mobility (Canada) cellular provider because they require the use of a http/https proxy.</p>
DEV-15031	Airwall Gateways	<p>Remote syslog over TLS doesn't work when using keys stored in TPM.</p>
DEV-14860	Conductor	<p>Airwall Gateways on older firmware (pre v2.2.0) may send passively-discovered device events to the Conductor even when the feature is off.</p>
DEV-14835	Conductor	<p>Airwall Gateway 150 serial numbers look like exponentiated numbers to Windows Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.</p>
DEV-14739	Airwall Gateways	<p>If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved.</p> <p>Workaround – If you need both IPv4 and IPv6, set static IP addresses for both.</p>
DEV-14736	Cellular Airwall Gateways	<p>Cellular details may display as "unavailable" on the first boot after you update an Airwall Gateway. The cellular connections are not affected.</p> <p>Workaround – Reboot the Airwall Gateway again to correctly display the cellular details.</p>
DEV-14726	Conductor	<p>If you're viewing an Android Airwall Agent Ports tab and the Airwall Agent changes how it's connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly.</p> <p>Workaround – Refresh the page.</p>
DEV-14715	macOS Airwall Agents	<p>Big Sur ARM64 Macs are not supported in this release</p>
DEV-14610	Conductor	<p>After changing the Reporting traffic stats reporting time, the CPU graph does not display.</p> <p>Workaround – Refresh your browser page.</p>

ID	Applies to	Description
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version v2.2.11 may not work.
		Workaround – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14570	Conductor	If you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 instead of a helpful error message.
DEV-14551	Conductor	The Android Airwall Agent lets you press the Edit Settings button on the Ports page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14308	OpenHIP	Initial packets are dropped while building a new tunnel to a new peer Airwall Gateway.
DEV-14249	iOS Airwall Agents	Check Secure Tunnels Tunnel Status may show as unavailable on iOS.
		Workaround – You can determine tunnel status by checking packets sent or received.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14045	Android and iOS Airwall Agents	iOS does not currently support overlay ping.
DEV-14015	OpenHIP	If an Airwall Relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay.
		Workaround – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13775	Azure Cloud Airwall Gateways	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13650	Conductor	SoIP device activity is not being reported on an Airwall Gateway Local Devices tab.

ID	Applies to	Description
DEV-13640	Conductor	Airwall Relay diagnostics don't work on a Standby Conductor.
DEV-13633	Conductor	A standby Conductor shows available firmware downloads, but they cannot be downloaded. Workaround – Download firmware from the active Conductor.
DEV-13620	Conductor	In Airwall > Ports > Failover settings , the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductor, Airwall Gateways	Creating a link failover group (Airwall > Ports > Failover settings) does not apply the settings to any port groups. You must also assign the failover group to port groups on the Ports page.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. Workaround – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13531	Cloud Conductor	Automatically creating Cloud HA Conductors only works if you use the same cloud provider for both active and standby Conductors. For example, AWS HA Active and AWS HA Standby. Workaround – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	If you configure multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then create a local device equal to the entire subnet with port affinity set, it may not lead to the expected result.
DEV-13331	Alibaba Cloud Airwall Gateways	The Alibaba Cloud Conductor system time is incorrect. Workaround – Change the Conductor system time to browser time: In Conductor Settings , under System time , select Edit Settings , select Set browser time , and then select Update Settings .
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." Workaround – Reboot and the details return.
DEV-13194	Conductor	Check Connectivity > Ping Local Devices for an Airwall Gateway fails in Internet Explorer 11 if one of the devices is defined as a CIDR. Workaround – Use one of the latest versions of Chrome, Firefox, Safari or Edge.

ID	Applies to	Description
DEV-11710	macOS Airwall Agents	If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly. Workaround – Close and reopen the macOS Airwall Agent.
DEV-10590	Cloud Airwall Gateways	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway-150 can show "could not detect attached switch" intermittently.
DEV-9546	Airwall Gateways, Airwall Gateways 150	The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.

Release Notes 2.2.13

Release Date: Jul 30, 2021

Update Considerations

Update to v2.2.13 if you want to use Advantech ICR-32xx model routers as Airwall Gateways.

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
•	Ran into these issues:

Downloads

For firmware and software downloads for this version, see [2.2.13 firmware and software](#) on page 434.

What's New in 2.2.13

Here are the new features and enhancements in this version.

Advantech Airwall Gateway

You can now use an Advantech ICR-32xx model router and install Airwall Gateway AV3200g firmware on it. The Advantech is a rugged form factor that you can install in harsher environments. The Advantech Airwall Gateway firmware supports Ethernet and Cell, as well as Serial port access and Serial over IP. It does not currently support Wifi or the second SIM socket. You must upgrade your Conductor to 2.2.13 to use the Advantech Airwall Gateway. If you're interested in this option, please contact Customer Success at support@tempered.io.

Learn more – [Set up Advantech hardware](#) on page 243

New and Improved Conductor Features

Port mirroring

Airwall Gateways configured with port mirroring now show mirrored status in list and status views.



DEV-15399

OpenID Connect

OpenID Connect tokens are now included in the webapp log at the debug level to assist with integration.

User Preferences

The Conductor now remembers user page size settings across sessions, browsers, and computers.

Underlay Network view

This view now visually separates the different underlay IPs to show their ping statuses, RTT, and count as they are being pinged.

Device name now shown on Overlay and Device pages

If you set a name for a device in an Airwall Agent or Server, it is now shown on the **Overlays** and **Devices** pages in the Conductor.

CPU Graph Changes

Starting with 2.2.12, the CPU graph on an Airwall Gateway Reporting page now shows CPU percentage, not the previously-shown CPU load average. The CPU percentage graph shows the percentage of CPU capacity being used on the Airwall Gateway over time.

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- [Diagrams for Port Mirroring](#)
- [Virtual Airwall Edge Services](#)

Updated –

- [How Airwall Licensing Works](#) on page 159
- [Set up a virtual Airwall Gateway in VMware ESX/ESXi](#) on page 259
- [Set up a virtual Airwall Gateway in Microsoft Hyper-V](#) on page 261
- [Alibaba Cloud – Set up an Airwall Gateway](#) on page 268
- [Amazon Web Services – Set up an Airwall Gateway](#) on page 273
- [Microsoft Azure – Set up an Airwall Gateway](#) on page 277
- [Google Cloud \(GCP\) – Set up an Airwall Gateway](#) on page 283
- [Airwall Gateway Airshell Console Commands - airsh](#) - New conf model command
- [Mirror Traffic to a Dedicated Port](#)

Fixes

ID	Applies to	Description
DEV-15984	Cellular Airwall Gateways	Fixed an issue that could block bypass traffic on cellular ports.
DEV-15948	Airwall Gateways	Fixed a DNS resolver issue that could cause long delays for Airwall Edge Services trying to reconnect to the Conductor that is configured with a hostname.
DEV-15880	Conductors	When you replace an Airwall Gateway, the Conductor now replaces port configurations of different Airwall Gateway models.
DEV-15839	Airwall Gateways	Fixed an issue that could impact overlay device connectivity.

Known Issues

ID	Applies to	Description
DEV-15987	Cellular Airwall Gateways	Using the "Check Bandwidth" function on the Secure Tunnels tab may cause the Advantech Airwall Gateway to lose access to its cell modem until a reboot.
DEV-15982	Conductors	Traffic stats reporting graphs generally show a smooth curve between data points. Over time the graph can show up with sharper angles. The data is still correct, but this is a known cosmetic issue.
DEV-15808	Google Cloud Airwall Gateways	In Google Cloud, use a unique deployment name (vm name) for Airwall Gateways. Airwall Gateways with the same vm name will have the same device serial number and this can result in a failure when you make a license request.
DEV-15791	Airwall Gateways	<p>On the Airwall Gateway-100, Port 2 might be inactive after a factory-reset.</p> <p>Workaround – Manually reboot the Airwall Gateway after a factory-reset.</p>
DEV-15787	OSX Airwall Agents	<p>Attempting to create a profile from the Remote Access User portal via the Request to connect to Conductor when a profile with that Conductor already exists will fail.</p> <p>Workaround -- Use an invite code or enter Conductor information manually.</p>
DEV-15705	Android and iOS Airwall Agents	<p>Establishing a tunnel TO a mobile agent (iOS / Android) will fail when there is no Airwall Relay involved.</p> <p>Workaround – Establish the tunnel FROM the mobile agent.</p>
DEV-15572	Airwall Gateways	Not specifying a gateway in DHCP server config causes the Airwall DHCP server to not include the DHCP Router option, so the DHCP client cannot configure a default gateway. Not specifying a gateway is an unusual config, and should only be used when you want to configure a single isolated subnet. For example, a subnet for networked PDUs that should not have any outside connectivity aside from remote access through an Airwall Gateway used in conjunction with SNAT over the overlay port group.
DEV-15489	Windows Airwall Agents and Servers	Windows 7 Users will see an extra Windows system popup when the UserAuth prompt appears on screen. This message can be safely ignored or the service can be disabled.
DEV-15381	Conductors	Sometimes, an Airwall Agent is not added to a Smart Device Group because the editor of the Smart Device Group rule does not have permissions to edit the Airwall Agent. This issue can happen, for example, when you add a tag to an Airwall Agent after it's been added to a single overlay network that the person who edited the rule is not a manager of. To avoid this issue, add tags relating to Smart Device Group actions to Airwall Agents and devices before adding them directly to any overlays.

ID	Applies to	Description
DEV-15357	macOS Airwall Agents	If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor.
		Workaround – Restart the agent or reapply the update.
DEV-15302	macOS Airwall Agents	The macOS Airwall Agent profile will not work correctly when restored to a new machine via Timemachine.
		Workaround – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one for that agent.
DEV-15219	MAP2-Client, OpenHIP	Airwall Gateways are not working on the Bell Mobility (Canada) cellular provider, due to the required use of a http/ https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14860	Conductors	Airwall Gateways on older firmware (pre 2.2.0) may send passively discovered device events to the Conductor even when the feature is off.
DEV-14835	Conductors	Airwall Gateway-150 serial numbers look like exponentiated numbers to Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14798	Conductors, Airwall Agents	Airwall Gateways with negative policy will still be able to talk to each other via their LSI. The peer will also still show up in the UI.
DEV-14772	macOS Airwall Agents	If the macOS Airwall Agent is set to "off on boot" and the computer is rebooted, DNS may not be correctly set at startup. Workaround – Restart the agent to regain access to DNS. Stop the agent, if desired, to return to the DNS servers as given by DHCP.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. Workaround – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update an Airwall Gateway. The cellular connections are not affected.
		Workaround – Reboot the Airwall Gateway again to correctly display the cellular details.

ID	Applies to	Description
DEV-14726	Conductor	If you're viewing an Android Airwall Gateway Ports tab and the Airwall Agent changes how it's connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly.
		Workaround – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph will not display.
		Workaround – Refresh your browser page.
DEV-14584	Cellular Airwall Gateways	Hot-swapping the SIM on an Airwall Gateway 110 with firmware version 2.2.11 may not work.
		Workaround – Reboot the Airwall Gateway after installing a new SIM card.
DEV-14570	Conductors	If you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 instead of a helpful error message.
DEV-14551	Conductors	The Android Airwall Agent lets you press the Edit Settings button on the Ports page; however, submitting any changes to the page results in an error message.
DEV-14426	Conductors, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14361	Airwall Gateways	The Build new tunnels if none exist option doesn't build tunnels to peer Airwall Edge Services with IPv6-only policy. This feature currently depends on having IPv4 policy between peer Airwall Edge Services.
DEV-14308	OpenHIP	Initial packets dropped while building a new tunnel to a new peer Airwall Edge Service.
DEV-14249	iOS Airwall Agents	Check Secure Tunnels / Tunnel Status may show as unavailable on iOS.
		Workaround – You can determine tunnel status by checking packets sent or received.
DEV-14223	Cloud-Google	Add an overlay IP to agent to talk to device behind Google Cloud Airwall Gateway 300v.
DEV-14218	Airwall Gateways	NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.

ID	Applies to	Description
DEV-14045	Android and iOS Airwall Agents	iOS does not currently support overlay ping. This feature may be implemented in a future release.
DEV-14015	OpenHIP	If a relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay. Workaround – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.
DEV-13760	Conductors	Device export/import does not export or import Bypass Devices.
DEV-13754	Airwall Agents and Servers	The Conductor can falsely report that the Airwall Agent is offline in some cases.
DEV-13699	Windows Airwall Agents and Servers	The initial ping from the Windows Airwall Agent can be misleading since it currently includes the time to initially set up the connection. Workaround – Ping a second time to see actual ping time.
DEV-13650	Conductors	SoIP device activity is not being reported on an Airwall Gateway Local Devices tab.
DEV-13640	Conductors	Airwall Relay diagnostics doesn't work on a Standby Conductor.
DEV-13633	Conductors	A standby Conductor shows available firmware downloads, but cannot be downloaded. Workaround – Download firmware from the active Conductor.
DEV-13620	Conductors	In Airwall > Ports > Failover settings , the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13607	Conductors, Airwall Gateways	Creating a link failover group (Airwall > Ports > Failover settings) does not apply the settings to any port groups. This is easy to miss since you have to set the failover group on the ports page.
DEV-13588	Conductors	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. Workaround – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13544	Linux Airwall Servers	If no relay is configured, checking Relay probe information on the Linux Airwall Server returns an error.

ID	Applies to	Description
DEV-13536	Windows Airwall Agents and Servers	<p>Uninstalling the Windows Airwall Agent does not remove the tun-tap driver.</p> <p>Workaround – Delete the driver from C:\Windows\System32\drivers\tnw-tap.sys.</p>
DEV-13531	Cloud	<p>Automating creating Cloud HA Conductors only works with same cloud provider used for both active and standby. For example, having both your HA Active and HA Standby Conductors in AWS.</p> <p>Workaround -- You can manually set up different cloud providers as HA pair Conductors.</p>
DEV-13474	Airwall Gateways	<p>Configuring multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then creating a local device equal to the entire subnet with port affinity set may not lead to the expected result.</p>
DEV-13331	Cloud-Alibaba	<p>Alibaba Cloud Conductor system time is incorrect.</p> <p>Workaround – Change the Conductor system time to browser time:</p> <ol style="list-style-type: none"> 1. In Conductor Settings, under System time, select Edit settings. 2. Select Set browser time, and then select Update.
DEV-13195	Conductors, Airwall Gateways	<p>When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become unavailable.</p> <p>Workaround – Reboot and the details return.</p>
DEV-13194	Conductors	<p>Check Connectivity / Ping Local Devices on an Airwall Gateway will fail in Internet Explorer 11 if one of the devices is defined as a CIDR.</p> <p>Workaround – use one of the latest versions of Chrome, Firefox, Safari or Edge.</p>

ID	Applies to	Description
DEV-12852	Windows Airwall Agents and Servers	<p>Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible.</p> <p>Workaround – Set Windows to keep multiple interfaces open by editing the fMinimizeConnections registry value:</p> <ol style="list-style-type: none"> 1. Hold the Windows key and press R. 2. In the Run dialog, type <code>regedit</code> and click OK. 3. Navigate to the following path in Registry Editor: <code>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\</code> 4. See if the GroupPolicy subkey exists. If not with, WcmSvc highlighted, right-click on WcmSvc and select New > Key, and name it GroupPolicy. 5. Right-click GroupPolicy and select New > DWORD(32-bit) > Create value. 6. Name the value fMinimizeConnections, and select OK. 7. Set the value to 0 (false). 8. Save, reboot, and test.
DEV-11710	macOS Airwall Agents	<p>If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly.</p> <p>Workaround – Close and reopen the macOS Airwall Agent.</p>
DEV-10590	Cloud	<p>The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.</p>
DEV-10039	Airwall Gateways	<p>An Airwall Gateway-150 can show a "Could not detect attached switch" message intermittently.</p>
DEV-9546	Airwall Gateways, Airwall Gateway-150	<p>The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.</p>

ID	Applies to	Description
DEV-9429	Windows Airwall Agents and Servers	Updating the Overlay Device IP address for a Windows Airwall Server in the Conductor doesn't update the first time. Workaround – Open and update the address a second time.

Release Notes 2.2.12 Hotfix – Conductor HF-15849

Release Date: Jun 17, 2021

This is a hotfix to release v2.2.12 for Conductors. See [Release Notes 2.2.12](#) on page 489 for more additions in this versions. Download 2.2.12 Conductor HF-1 from [Hotfixes](#) on page 454.

Update Considerations

Update to this v2.2.12 Conductor hotfix if you:

-

Fixes

ID	Applies to	Description
DEV-	Conductor	

Known Issues

See [Release Notes 2.2.12](#) on page 489 for known issues.

Release Notes 2.2.12 Hotfix – Conductor HF-15748

Release Date: May 28, 2021

This is a hotfix to release v2.2.12 for Conductors. See [Release Notes 2.2.12](#) on page 489 for more additions in this versions. Download 2.2.12 Conductor HF-15748 from [Hotfixes](#) on page 454.

Update Considerations

Update to this v2.2.12 Conductor hotfix if you:

- Replace the port configuration of different Airwall Gateways.

Fixes

ID	Applies to	Description
DEV-15748	Conductor	Hotfix that allows replacing port configuration of different Airwall Gateways.

Known Issues

See [Release Notes 2.2.12](#) on page 489 for known issues.

Release Notes 2.2.12

Release Date: May 24, 2021

Update Considerations

Consider updating to v2.2.12 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
<ul style="list-style-type: none"> • Use a Raspberry Pi as an Airwall Server • Plan on installing an 8-port module in an already in production Airwall Gateway-500 	<p>Ran into these issues:</p> <ul style="list-style-type: none"> • Had issues with reconnecting previously revoked devices • Issues with Bypass in certain cases • Issues with port mirroring after deleting a destination • Have issues with Bypass and Device Discovery

Downloads

For firmware and software downloads for this version, see [2.2.12 firmware and software](#) on page 436.

What's New in 2.2.12

Here are the new features and enhancements in this version.

Licensing Changes

- Port mirroring now requires an add-on license for any Airwall Gateway acting as a Mirror Source
- Licensing page changes:
 - Licenses are now paginated as needed.
 - Vouchers are automatically consolidated

Airwall Servers for Raspbian and Ubuntu ARM64

You can now get an Airwall Server that runs on Raspbian or Ubuntu ARM. For installation information, see [Raspbian and RPi4/Ubuntu ARM64 – Install the Airwall Server](#) on page 11.

Platform End of Life for 100 Series Appliances

Tempered announces the End of Life schedule for the HIPswitch 100 series platforms. For more information and a schedule, see [Platform end-of-life for Airwall Gateway/ HIPswitch 100 series](#) on page 423.

New and Improved Conductor Features

Port mirroring

Airwall Gateways configured with port mirroring now show mirrored status in list and status views.



DEV-15399

OpenID Connect

OpenID Connect tokens are now included in the webapp log at the debug level to assist with integration.

User Preferences

The Conductor now remembers user page size settings across sessions, browsers, and computers.

Underlay Network view

This view now visually separates the different underlay IPs to show their ping statuses, RTT, and count as they are being pinged.

Device name now shown on Overlay and Device pages If you set a name for a device in an Airwall Agent or Server, it is now shown on the **Overlays** and **Devices** pages in the Conductor.

CPU Graph Changes

Starting with 2.2.12, the CPU graph on an Airwall Gateway Reporting page now shows CPU percentage, not the previously-shown CPU load average. The CPU percentage graph shows the percentage of CPU capacity being used on the Airwall Gateway over time.

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- [Diagrams for Port Mirroring](#)
- [Virtual Airwall Edge Services](#)

Updated –

- [How Airwall Licensing Works](#) on page 159
- [Set up a virtual Airwall Gateway in VMware ESX/ESXi](#) on page 259
- [Set up a virtual Airwall Gateway in Microsoft Hyper-V](#) on page 261
- [Alibaba Cloud – Set up an Airwall Gateway](#) on page 268
- [Amazon Web Services – Set up an Airwall Gateway](#) on page 273
- [Microsoft Azure – Set up an Airwall Gateway](#) on page 277
- [Google Cloud \(GCP\) – Set up an Airwall Gateway](#) on page 283
- [Airwall Gateway Airshell Console Commands - airsh](#) - New conf model command
- [Mirror Traffic to a Dedicated Port](#)

Fixes

ID	Applies to	Description
DEV-16133	Windows Airwall Agents and Servers	Fixed an issue where Windows Airwall Agents and Servers sometimes lock up.
DEV-16101	Windows Airwall Agents and Servers	Fixed an issue where a Windows Airwall Agent or Server loses connectivity with the Conductor, or where the agent is still connected but cannot establish communications.
DEV-15680	Airwall Gateways	The Airwall Gateway CPU Load graph has been revised for Airwall Gateways running v2.2.12 and later. This graph now reports the percentage of CPU used rather than the load average reported by previous releases.
DEV-15635	Conductors	Fixed an issue where read-only system administrators were prevented from seeing license counts.
DEV-15579	Conductors	Fixed an issue where an incorrect packet capture interface may get selected when using Firefox browser.
DEV-15563	Conductors	Fixed an issue where the GRE key field wasn't being published for port mirror destinations.
DEV-15543	Conductors	Fixed an issue where group validation fails if there is a comma in the group name.

ID	Applies to	Description
DEV-15541	macOS Airwall Agents	Fixed an issue where the macOS Airwall Agent wasn't cleaning up routes when shut down.
DEV-15538	Conductors	Fixed an issue where you could not add a device group with bypass destinations to an overlay.
DEV-15503	Airwall Gateways	Fixed an issue where Airwall Gateways were not always broadcasting all their monitor capabilities.
DEV-15467	Conductors	Swapping between Airwall Gateways should correctly reset the owner setting
DEV-15448	API, Conductors	API for port mirrors incorrectly used enumerable ID. It now uses a UUID.
DEV-15444	Conductors	Fixed an issue that could cause the Conductor to refuse policy creation involving bypass destinations in some situations.
DEV-15385	Airwall Gateways	Fixed an issue that could cause bad port and network configurations on Airwall Gateways with port expansion capabilities after inserting a network expansion module.
DEV-15378	Airwall Gateways	Fixed an issue where you had to remove the Port Mirroring config before deleting a device.
DEV-15374	Android and iOS Airwall Agents	Airwall Agents now automatically restart when the port for HIP is changed on Conductor.
DEV-15370	Airwall Gateways	Fixed passive device discovery on routed traffic only port groups.
DEV-15367	Conductors	The user is now blocked from completing user auth if they are within a negative access window on any people group.
DEV-15360	Airwall Gateways	Fixed an issue where the port 1 and 2 labels were swapped on an AW-100 after it has been factory reset.
DEV-15352	Conductors	Fixed a UI issue that prevented changes to bypass settings on a standby Conductor.
DEV-15348	Conductors	The ping peer Airwalls diagnostic function in the UI should now enable/disable dynamically as the Airwall gains or loses peers.
DEV-15341	Airwall Gateways	Fixed an ebm2 crash on a rare race condition encountered when updating ports configuration when port mirroring is enabled.
DEV-15316	Airwall Gateways	Fixed an issue that caused Ping peer Airwalls to report a failure sending HIP traffic for HA-configured Airwall Gateways.
DEV-15314	Conductors	Fixed an issue where when using user auth tags and access windows, a user logging in could gain transient (< 5 minutes) access to a tag when they are outside the access window, and therefore gain access to a resource via smart device groups when they should not. Also fixed an issue where when a user gains a user auth tag that is in multiple people groups with access windows, the user might only gain access for the shorter window depending on group ordering.

ID	Applies to	Description
DEV-15305	Conductors	The Conductor now validates the local device MAC address is a unicast address.
DEV-15179	HIP tunnel, Diagnostic mode	Fixed an issue where 'airsh conf cell roaming=1' did not match Diagnostic Mode settings. New syntax is 'airsh conf cell roaming=true' (or '... roaming=false').
DEV-15005	Conductors, Android Airwall Agents	Fixed an issue where overlay stats were not showing on the Android Airwall Agent.
DEV-14994	Android Airwall Agents	Fixed an issue where the cell port temporarily didn't show up on the Ports page in Conductor for an Android Airwall Agent.
DEV-14990	Airwall Gateways	Fixed an issue where bypass policy was applied to outbound but not inbound traffic.
DEV-14952	Airwall Agents and Servers	Fixed an issue where the Android Airwall Agent was not able to ping peer devices on Airwall Teams unless the communication was initiated from the peer devices.
DEV-14917	Android Airwall Agents	Fixed an issue where you couldn't stop the packet capture for Android Airwall Agents.
DEV-14874	Android Airwall Agents	Fixed an issue where the Android Airwall Agent was reporting the underlay IP as 0.0.0.0 when on cellular.
DEV-14816	Conductors, Android and iOS Airwall Agents	The UI for the mobile agents need to be in either the background or foreground for the change to take effect without user interaction.
DEV-14806	Android Airwall Agents	Fixed an issue where Android 6 & 7 devices were unable to ping peer device without an Overlay device IP set.
DEV-14800	Android Airwall Agents	If an Android has multiple underlay IP addresses (like IPv4 and IPv6), the Conductor now pings them separately.
DEV-14795	Android Airwall Agents	Reduced the timeout length for Check secure tunnel on the Conductor for Android Airwall Agents.
DEV-14794	Android Airwall Agents	Fixed an issue where Check secure tunnel on the Conductor was not working on older Android devices.
DEV-14771	Android Airwall Agents	Note that if you scroll to the top while the log viewer is scrolling it will not force you to the bottom. It will only auto-scroll if you are scrolled to the last line and new log messages come in, which is how most auto-scrolling works.
DEV-14758	Conductors, Android Airwall Agents	Fixed an issue where the Conductor was sometimes not showing an IP for Android Airwall Agents.
DEV-14683	Airwall Gateways	Fixed an issue causing missing ports in the selection dropdown of the packet capture dialog of newly managed Airwall Edge Services.
DEV-14509	Airwall Gateways	Ping peer Airwalls (under Diagnostics > Check connectivity > Airwall peer connectivity) was fixed for Airwall Gateways and Linux Airwall Servers. Note that the other Airwall Agents and Servers (Windows, macOS, iOS, Android) may display a green checkboxes under HIP traffic when a HIP tunnel may not actually be available (false positives).

Known Issues

ID	Applies to	Description
DEV-16107	Windows Airwall Agents and Servers	<p>There is an issue on Windows Airwall Agents and Servers where when you set the log level, the agent loses its connection to the Conductor, and no longer writes anything to the log.</p> <p>Workaround: Change the log level again, or close and restart the Airwall Agent or Server.</p>
DEV-15808	Google Cloud Airwall Gateways	<p>In Google Cloud, use a unique deployment name (vm name) for Airwall Gateways. Airwall Gateways with the same vm name will have the same device serial number and this can result in a failure when you make a license request.</p>
DEV-15803	Conductors	<p>When you replace an Airwall Gateway in the Conductor, it transfers the Underlay IP (NAT) during the Transfer port configuration step, even if you haven't checked Transfer public IP addresses.</p> <p>Workaround – Update the Underlay IP (NAT) after completing the Airwall replace.</p>
DEV-15791	Airwall Gateways	<p>On the Airwall Gateway-100, Port 2 might be inactive after a factory-reset.</p> <p>Workaround – Manually reboot the Airwall Gateway after a factory-reset.</p>
DEV-15705	Android and iOS Airwall Agents	<p>Establishing a tunnel TO a mobile agent (iOS / Android) will fail when there is no Airwall Relay involved.</p> <p>Workaround – Establish the tunnel FROM the mobile agent.</p>
DEV-15489	Windows Airwall Agents and Servers	<p>Windows 7 Users will see an extra Windows system popup when the UserAuth prompt appears on screen. This message can be safely ignored or the service can be disabled.</p>
DEV-15357	macOS Airwall Agents	<p>If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor.</p> <p>Workaround – Restart the agent or reapply the update.</p>
DEV-15302	macOS Airwall Agents	<p>The macOS Airwall Agent profile will not work correctly when restored to a new machine via Timemachine.</p> <p>Workaround – Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one for that agent.</p>

ID	Applies to	Description
DEV-15219	MAP2-Client, OpenHIP	Airwall Gateways are not working on the Bell Mobility (Canada) cellular provider, due to the required use of a http/https proxy.
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM.
DEV-14892	Android Airwall Agents	Network order for Ethernet connections on an Android Airwall Agent doesn't work.
DEV-14835	Conductors	Airwall Gateway-150 serial numbers look like exponentiated numbers to Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14798	Conductors, Airwall Agents	Airwall Gateways with negative policy will still be able to talk to each other via their LSI. The peer will also still show up in the UI.
DEV-14772	macOS Airwall Agents	If the macOS Airwall Agent is set to "off on boot" and the computer is rebooted, DNS may not be correctly set at startup. Workaround – Restart the agent to regain access to DNS. Stop the agent, if desired, to return to the DNS servers as given by DHCP.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. Workaround – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update an Airwall Gateway. The cellular connections are not affected. Workaround – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you're viewing an Android Airwall Gateway Ports tab and the Airwall Agent changes how it's connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly. Workaround – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph will not display. Workaround – Refresh your browser page.

ID	Applies to	Description
DEV-14584	Cellular Airwall Gateways	<p>Hot-swapping the SIM on an Airwall Gateway 110 with firmware version 2.2.11 may not work.</p> <p>Workaround – Reboot the Airwall Gateway after installing a new SIM card.</p>
DEV-14570	Conductors	<p>If you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 instead of a helpful error message.</p>
DEV-14551	Conductors	<p>The Android Airwall Agent lets you press the Edit Settings button on the Ports page; however, submitting any changes to the page results in an error message.</p>
DEV-14426	Conductors, Airwall Gateways	<p>Bypass destinations with a hostname do not show device activity in the Conductor.</p>
DEV-14361	Airwall Gateways	<p>The Build new tunnels if none exist option doesn't build tunnels to peer Airwall Edge Services with IPv6-only policy. This feature currently depends on having IPv4 policy between peer Airwall Edge Services.</p>
DEV-14308	OpenHIP	<p>Initial packets dropped while building a new tunnel to a new peer Airwall Edge Service.</p>
DEV-14249	iOS Airwall Agents	<p>Check Secure Tunnels / Tunnel Status may show as unavailable on iOS.</p> <p>Workaround – You can determine tunnel status by checking packets sent or received.</p>
DEV-14223	Cloud-Google	<p>Add an overlay IP to agent to talk to device behind Google Cloud Airwall Gateway 300v.</p>
DEV-14218	Airwall Gateways	<p>NAT broadcast applied to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.</p>
DEV-14045	Android and iOS Airwall Agents	<p>iOS does not currently support overlay ping. This feature may be implemented in a future release.</p>
DEV-14015	OpenHIP	<p>If a relay is also used as a bypass gateway, Airwall Edge Services behind the relay are not able to use that relay.</p> <p>Workaround – Deploy multiple relays so at least one relay is usable by each pair of Airwall Edge Services that need to communicate.</p>

ID	Applies to	Description
DEV-13970	Cloud-Alibaba, Conductors	<p>When you upgrade a Conductor on Alibaba Cloud, the Conductor system time gets out of sync.</p> <p>Workaround – Go to Settings > Other settings > System time and date, click Edit Settings, then Update to resync.</p>
DEV-13775	Cloud-Azure	<p>The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.</p>
DEV-13760	Conductors	<p>Device export/import does not export or import Bypass Devices.</p>
DEV-13754	Airwall Agents and Servers	<p>The Conductor can falsely report that the Airwall Agent is offline in some cases.</p>
DEV-13699	Windows Airwall Agents and Servers	<p>The initial ping from the Windows Airwall Agent can be misleading since it currently includes the time to initially set up the connection.</p> <p>Workaround – Ping a second time to see actual ping time.</p>
DEV-13650	Conductors	<p>SoIP device activity is not being reported on an Airwall Gateway Local Devices tab.</p>
DEV-13640	Conductors	<p>Airwall Relay diagnostics doesn't work on a Standby Conductor.</p>
DEV-13633	Conductors	<p>A standby Conductor shows available firmware downloads, but cannot be downloaded.</p> <p>Workaround – Download firmware from the active Conductor.</p>
DEV-13620	Conductors	<p>In Airwall > Ports > Failover settings, the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.</p>
DEV-13607	Conductors, Airwall Gateways	<p>Creating a link failover group (Airwall > Ports > Failover settings) does not apply the settings to any port groups. This is easy to miss since you have to set the failover group on the ports page.</p>
DEV-13588	Conductors	<p>Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments.</p> <p>Workaround – Use the latest version of Chrome, Firefox, or Edge instead.</p>
DEV-13544	Linux Airwall Servers	<p>If no relay is configured, checking Relay probe information on the Linux Airwall Server returns an error.</p>

ID	Applies to	Description
DEV-13536	Windows Airwall Agents and Servers	<p>Uninstalling the Windows Airwall Agent does not remove the tun-tap driver.</p> <p>Workaround – Delete the driver from C:\Windows\System32\drivers\tnw-tap.sys.</p>
DEV-13531	Cloud	<p>Automating creating Cloud HA Conductors only works with same cloud provider used for both active and standby. For example, having both your HA Active and HA Standby Conductors in AWS.</p> <p>Workaround -- You can manually set up different cloud providers as HA pair Conductors.</p>
DEV-13474	Airwall Gateways	<p>Configuring multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then creating a local device equal to the entire subnet with port affinity set may not lead to the expected result.</p>
DEV-13331	Cloud-Alibaba	<p>Alibaba Cloud Conductor system time is incorrect.</p> <p>Workaround – Change the Conductor system time to browser time:</p> <ol style="list-style-type: none"> 1. In Conductor Settings, under System time, select Edit settings. 2. Select Set browser time, and then select Update.
DEV-13195	Conductors, Airwall Gateways	<p>When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become unavailable.</p> <p>Workaround – Reboot and the details return.</p>
DEV-13194	Conductors	<p>Check Connectivity / Ping Local Devices on an Airwall Gateway will fail in Internet Explorer 11 if one of the devices is defined as a CIDR.</p> <p>Workaround – use one of the latest versions of Chrome, Firefox, Safari or Edge.</p>

ID	Applies to	Description
DEV-12852	Windows Airwall Agents and Servers	<p>Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible.</p> <p>Workaround – Set Windows to keep multiple interfaces open by editing the fMinimizeConnections registry value:</p> <ol style="list-style-type: none"> 1. Hold the Windows key and press R. 2. In the Run dialog, type <code>regedit</code> and click OK. 3. Navigate to the following path in Registry Editor: <code>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\</code> 4. See if the GroupPolicy subkey exists. If not with, WcmSvc highlighted, right-click on WcmSvc and select New > Key, and name it GroupPolicy. 5. Right-click GroupPolicy and select New > DWORD(32-bit) > Create value. 6. Name the value fMinimizeConnections, and select OK. 7. Set the value to 0 (false). 8. Save, reboot, and test.
DEV-11710	macOS Airwall Agents	<p>If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly.</p> <p>Workaround – Close and reopen the macOS Airwall Agent.</p>
DEV-10590	Cloud	<p>The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.</p>
DEV-10039	Airwall Gateways	<p>An Airwall Gateway-150 can show a "Could not detect attached switch" message intermittently.</p>
DEV-9546	Airwall Gateways, Airwall Gateway-150	<p>The Airwall Gateway-150 serial connection has an intermittent issue when large amounts of data are sent over the console.</p>

ID	Applies to	Description
DEV-9429	Windows Airwall Agents and Servers	Updating the Overlay Device IP address for a Windows Airwall Server in the Conductor doesn't update the first time. Workaround – Open and update the address a second time.

Release Notes 2.2.11 Hotfix – Conductor HF-1

Release Date: Apr 13, 2021

This is a hotfix to release v2.2.11 for Conductors. See [Release Notes 2.2.11](#) on page 502 for more additions in version 2.2.11. Download 2.2.11 Conductor HF-1 from [Hotfixes](#) on page 454.

Update Considerations

Update to this 2.2.11 Conductor hotfix if you:

- Want to use device groups for bypass devices
- Want to use GRE keys to disambiguate mirrored traffic
- Have an Airwall Gateway reporting bypass not enabled after enabling
- Cannot select all Airwall Gateways when creating link failover events

Fixes

ID	Applies to	Description
DEV-15577	Conductor	Fixed an issue where a Device Group with more than two DNS Bypass Destinations could not be added to an Overlay Network.
DEV-15564	Conductor	Fixed an issue where the GRE key field wasn't being published for port mirror destinations.
DEV-15552	Conductor	Full OpenID Connect tokens are printed in the webapp log at debug level to make it easier to integrate Conductor with OIDC providers.
DEV-15545	Conductor	LDAP and OpenID Connect groups containing commas are now supported. Commas in group names can now be escaped if used. For example, enter 123\,foo, 456\,bar to match groups 123,foo and 456,bar.
DEV-15542	Conductor	Fixed an issue that could cause the Conductor to reject policies with a bypass destination in some situations.
DEV-15524	Airwall Gateways	Fixed an issue where Airwall Gateways were sometimes not broadcasting all of their monitor capabilities.
DEV-15415	Conductor	If a user is blocked by any Access window in any people group, they are now blocked from completing user auth.
DEV-15380	Conductor	Fixed an issue where deleting a device that is being used as a port mirroring destination could prevent port mirroring config changes on that Airwall Gateway.

Known Issues

See [Release Notes 2.2.11](#) on page 502 for known issues.

Release Notes 2.2.11 Hotfix – Airwall Gateway HF-2

Release Date: Mar 30, 2021

This is a hotfix to release v2.2.11 for Airwall Gateways. See [Release Notes 2.2.11](#) on page 502 for more additions in version 2.2.11. Download HF-2 from [Hotfixes](#) on page 454.

Upgrade Considerations

Upgrade to this 2.2.11 Airwall Gateway hotfix if you ran into issues where traffic to bypass destinations did not work as expected.

Fixes

ID	Applies to	Description
DEV-15479	Airwall Gateway	Fixed an issue where devices with policy on an underlay bypass port did not create routes.

Known Issues

See [Release Notes 2.2.11](#) on page 502 for known issues.

Release Notes 2.2.11 Hotfix – Airwall Gateway HF-1

Release Date: Mar 17, 2021

This is a hotfix to release v2.2.11 for Airwall Gateways. See [Release Notes 2.2.11](#) on page 502 for more additions in version 2.2.11. Download HF-1 from [Hotfixes](#) on page 454.

Upgrade Considerations

Upgrade to this 2.2.11 Airwall Gateway hotfix if you were experiencing any of the following issues:

- Passive device discovery wasn't working on Routed traffic only port groups.
- Installing an expansion module mixed up ports.
- You had issues when using both Seamless bypass and port mirroring

Fixes

ID	Applies to	Description
DEV-15402	Airwall Gateway	Fixed using bypass and port mirroring port group destination concurrently.
DEV-15392	Airwall Gateway	Fixed passive device discovery on routed traffic only port groups.
DEV-15391	Airwall Gateway	Fixed rare crash when updating ports configuration while port mirroring is enabled.
DEV-15379	Airwall Gateway	Fixed an issue where an Airwall Gateway is unable to synchronize with the Conductor after port mirroring destination device is deleted followed by a reboot of the Airwall Gateway.
DEV-15324	Airwall Gateway	Fixed expansion module detection and issue where ports were mixed up after installing an expansion module.

Known Issues

See [Release Notes 2.2.11](#) on page 502 for known issues.

Release Notes 2.2.11

Release Date: Mar 15, 2021

What's New in 2.2.11

Here are the new features and enhancements in this version.

Mirror network traffic for Packet Analyzers

You can now mirror network traffic to packet analyzer/visibility tools (like Nozomi or Wireshark) to see what's going on in your Airwall secure network.

See more: [Mirror traffic from your Airwall Gateways to a packet analyzer tool](#) on page 389

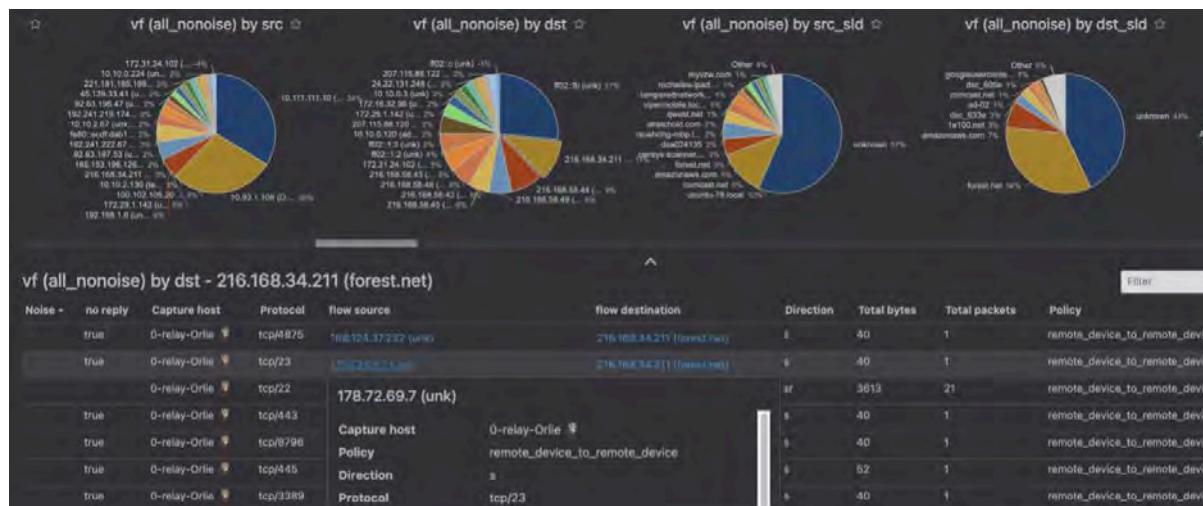
Assign Separate DNS Servers to Airwall Agents and Servers

If you need Airwall Agents and Servers to use different DNS servers, you can assign different DNS servers on an Overlay or individually for Airwall Agents and Servers that support it.

See more: [Assign Separate DNS Servers to Airwall Agents and Servers](#) on page 296

Preview - Airwall Visibility Connector

The Airwall Visibility Connector gives you a dynamic L4 view into the health and status of your Airwall secure network. You can explore many pre-computed reports in the Conductor, and can integrate other threat detection platforms. When configured, the Conductor continuously learns from these external systems, and can report or respond to threats as they are detected.



Contact Customer Success at support@tempered.io if you would like to preview this feature. A future version will expose the full feature with appropriate documentation, training, and platform options.

Raspberry Pi Airwall Agent

You can now get an Airwall Agent that runs on Raspberry Pi. For information, see .

Platform End of Life for 100 Series Appliances

Tempered announces the End of Life schedule for the HIPswitch 100 series platforms. For more information and a schedule, see [Platform end-of-life for Airwall Gateway/ HIPswitch 100 series](#) on page 423.

New Knowledge Base and Support Site

Tempered has a new site for our product Knowledge Base articles and support. Update your links!

- New Link to open a Support ticket: <https://www.tempered.io/support/supportReq.html>
- New location for Knowledge Base articles: <https://tempered.force.com/TemperedSupportCenter/s/>

New and Improved Conductor Features

Update macOS Airwall Agents from the Conductor

In v2.2.11, the macOS Airwall Agent introduces the ability to update from a Conductor package. For those running v2.2.10, upgrade one last time manually, with:

```
sudo installer -pkg /path/to/
Airwall-Mac_2.2.11.xxxx.pkg -
target /
```

You can then update future versions from a Conductor update package.

DEV-14804

Clear Recent events on the Dashboard

On the Dashboard System navigation, you can clear all events by selecting the Dismiss events icon :

DEV-15157

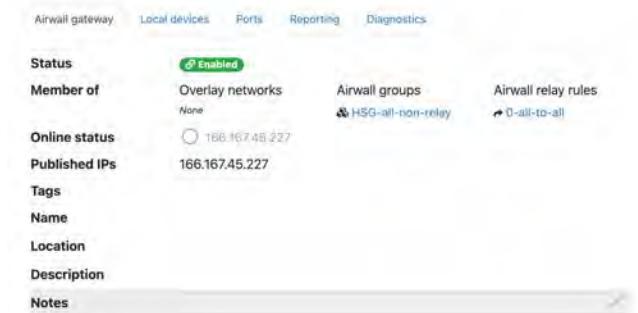
Recent events

New Airwall online 1710250K0182 Airwall-250gd View Manage	New provisioning request 7A9BBE687739 Airwall-300v View	New provisioning request 138BE3353252 Airwall-300v View	New provisioning re... 08C1E0989CE2 airwall-linux-0cfba... Airwall-Linux View
--	--	--	--

New Notes field on Airwall Edge Service pages

There is now a place where administrators can add notes on Airwall Edge Service pages: DEV-15111

Airwall gateway - 10192010007D



The screenshot shows the 'Airwall gateway' configuration page. At the top, there are tabs for 'Airwall gateway', 'Local devices', 'Ports', 'Reporting', and 'Diagnostics'. Below the tabs, there are several sections with configuration options. One section is labeled 'Status' with a 'Enabled' button. Another section is 'Member of' with 'Overlay networks' set to 'None'. Under 'Online status', it shows '166.167.48.227'. In the 'Published IPs' section, the IP address '166.167.45.227' is listed. There are also sections for 'Tags', 'Name', 'Location', 'Description', and 'Notes'. The 'Notes' section is currently empty.

Conductor theme now follows you

Your Conductor theme is now saved across computers and browsers. DEV-15022

Failover groups improvement

Failover groups now start with an initial likely selection for underlay link failover configuration. DEV-14900

OpenID Connect improvement

OpenID Connect now supports Azure Active Directory (AD). DEV-14864

Conductor Certificate Expiration reminders

When a Conductor certificate is near expiration (1 month + 1 week), you get an event and a tag on the cert info that warns you of the upcoming expiration. On the day of

Download a CSV with Licensing and Airwall Data

expiration, you get an alert, event, and a tag telling you the certificate has expired. DEV-15160

Access Windows Date Selection improvements

You can download all licensing and Airwall data in CSV format from **Settings > Licensing**. This data can be helpful in ensuring your Conductor vouchers are correctly renewed. DEV-14869

Airshell Improvements

The way you choose dates for Access windows has been improved. DEV-14649

Alert Improvements

You can now save your network configuration when doing a factory reset using the keep-networking option. See [Airwall Gateway Airshell console commands – airsh](#) on page 305. DEV-14465

Diagnostic Mode Improvements

Intrusion prevention alerts now indicate which devices are the source or destination of the alert where possible. These alerts are in Conductor alerts and indicated by the ID in the event data from the API DEV-14502, and snort metadata will be included in the API. DEV-14490

API Improvements

- Diagnostic Report Addition – The Diagnostic report now includes policy-based routing rules and IPv6 routes. DEV-14720
- Return to Diag mode after a hotfix – When applying a hotfix that does not require reboot, when the hotfix is complete you get an option to return to Diag mode. DEV-14582
- API tracks when changes happened – The Conductor API now serializes when many resources were created and updated, and includes These changes make it easier to see when resources were added or have changed from the API. DEV-14962
- New API endpoints – New API endpoints show history of Airwall Edge Services being managed and revoked DEV-15113, and returns a list of devices that each device has policy to and what overlays the policies are in DEV-14717.
- Date time/NTP settings – The API now allows updating of Date time/NTP settings. DEV-14716

New and Updated Help

In addition to the content added for new features linked above, here's the new and updated content published since our last major release:

New –

- [Configure an Underlay Port Failover Group](#)
- [Best Practices for Underlay Port Failover Groups](#)

Updated –

- [Seamless Bypass](#)

Introducing our new free offering – Airwall Teams

Airwall Teams allows you to build truly private system-to-system networks—that span public, private, cloud, and mobile networks using an intuitive graphical interface - just draw lines between devices you want to connect. Airwall Teams replaces and expands on our Airnet platform.

See more:

- [Sign up – Airwall Teams](#)
- [Check out the help – Airwall Teams Help](#)

Update Considerations

Consider updating to v2.2.11 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
<ul style="list-style-type: none"> • Mirror network traffic to a packet analyzer • Assign different DNS servers to Airwall Agents and Servers 	<p>Ran into these issues:</p> <ul style="list-style-type: none"> • Syslog issues – User Authentication was logging to Syslog, and external syslog over TLS • Seeing high CPU use from logwatch • Airwall Invitations were incorrectly using the US date format

Downloads

For firmware and software downloads for this version, see [2.2.11 firmware and software](#) on page 437.

Fixes

ID	Applies to	Description
DEV-15317	Conductor	When using user authentication access windows, sessions now end at the end of the session timeout of the Airwall Edge Service if it is shorter than the access window.
DEV-15307	Linux Airwall Servers	Fixed some DNS issues in Linux Airwall Servers.
DEV-15265	Airwall Gateway	Fixed an issue where taking a packet capture didn't include hipbrN interfaces in Routed only overlay port groups.
DEV-15206	Conductor	When you attempt to disable a user who is the owner of any smart device groups, the Conductor now shows a warning advising you to transfer ownership to avoid their smart device groups being downgraded to regular device groups.
DEV-15152	Conductor	Fixed an issue where there could be unidentified device activity in the log.
DEV-15045	Windows Airwall Agents and Servers	Fixed an issue that caused the Windows Airwall Agents and Servers to close unexpectedly.
DEV-15001	macOS Airwall Agents	Fixed an issue where Okta user authentication was failing when you had assigned DNS servers globally on macOS Airwall Agents.

ID	Applies to	Description
DEV-14996	macOS Airwall Agents	macOS Airwall Agents now correctly install on Big Sur (version 11.x) without excessive prompts to accept certificates.
DEV-14983	Conductor	When using the device discovered monitor with the tag action, tags are now correctly added to the discovered device, not the Airwall Gateway with the device.
DEV-14981	Linux Airwall Servers	Fixed an issue where occasionally ping results were not returned.
DEV-14980	Linux Airwall Servers	When attempting to connecting to the Conductor, if an error occurs, the Linux Airwall Servers now moves to the next network interface and tries again.
DEV-14976	Common	Fixed remote syslog to a TLS 1.3 endpoint.
DEV-14975	Windows Airwall Agents and Servers	Customers are unable to view Devices in the HIP Networks View portion of Windows Airwall Agents and Servers.
DEV-14972	Conductor	Resolved a display issue in the throughput shown on the Conductor Dashboard where bars would overlap with the legend.
DEV-14971	Cellular Airwall Gateways	Fixed a regression that sometimes caused long wait times when connecting an Airwall Gateway 110g to Verizon.
DEV-14958	Cloud-Azure, Conductor	Saving the Azure Conductor template with a new resource group name now appears correctly when you edit the template again.
DEV-14956	Airwall Gateways	Fixed a crash when using hostname based policy.
DEV-14951	Conductor, Airwall Gateways	Fixed an issue that could cause a database migration to fail on upgrade.
DEV-14922	Conductor	Fixed an issue where people groups integration with authentication providers (LDAP or OpenID Connect) could run into problems if there were groups with the same name with different capitalization.
DEV-14893	Windows Airwall Agents and Servers	Fixed an issue where you had to disable lockdown mode on 2.2.10 Windows Airwall Agents and Servers before stopping it for traffic to properly pass.
DEV-14891	Conductor	Read-only administrators can now see e-mail addresses in user settings.
DEV-14888	Conductor	Syslog now includes remote session (login via agent / server) creation, failed attempts, and termination.
DEV-14887	Conductor	Fixed an issue where in some cases a failed OpenID Connect login could result in a 500 error.
DEV-14878	Linux Airwall Servers	Linux Airwall Servers now keep full firmware install logs.
DEV-14875	Cellular Airwall Gateways	Fixed an issue where Airwall Gateway 150s would sometimes experience 100% CPU usage when a remote syslog server was configured.

ID	Applies to	Description
DEV-14872	Conductor	Fixed an issue where the link to set your password for a new user that is provided by email expired very quickly, and certain password error messages were not being displayed on the reset password page.
DEV-14863	Conductor	Licensing tab is now more clear about when your licenses will expire.
DEV-14854	Conductor	Fixed an issue where the remote access user portal's Linux Airwall Server connection string was missing the activation code.
DEV-14852	Linux Airwall Servers	Fixed a bug that could cause excessive numbers of Airwall interface status updates.
DEV-14848	Airwall Gateways	Fixed an issue that could cause the root file system to fill up with log messages on some virtual platforms.
DEV-14822	Conductor	Airwall Invitations now correctly honor local time and date format.
DEV-14820	Android, iOS, macOS, and Linux Airwall Agents and Servers	Airwall Agents and Servers now automatically restart when the port for HIP is changed on Conductor.
DEV-14803	Conductor	Fixed an issue that caused the logging settings for the Conductor to be ignored for the syslog output.
DEV-14766	Airwall Teams, Conductor	The Airwall Invitation API now returns the activation code in its response.
DEV-14725	Conductor	The Overlay network page where you manage devices and device groups now filters bypass destinations under their own heading.
DEV-14723	Conductor	On the Detect devices page, the networks under Network to scan are now normalized. For example, '192.168.1.0/24' instead of '192.168.1.1/24'
DEV-14722	Conductor	When you delete a device from an overlay network that uses managed relay rules, if the Airwall Edge Service that device was on has no other devices in the overlay, then the Airwall Edge Service is now also removed from the managed relay rule.
DEV-14713	Conductor	The Conductor now correctly displays IPv6 addresses in Bypass settings.
DEV-14692	Airshell	In the new Airshell 'conf network' menu, when editing a port group, it is possible to enter invalid or duplicate interfaces, or interfaces already in use by another port group. When entering interface names, use 'status network' output to see current settings and avoid invalid configurations.
DEV-14690	Airshell	The Airshell command, 'conf network', now lists available interfaces when assigning interfaces to a port group.
DEV-14689	Airshell	Fixed an issue where Airshell "conf network" would time out when applying changes, even though settings were saved.

ID	Applies to	Description
DEV-14688	Cellular Airwall Gateways	The APN setting is now retained when you factory reset an Airwall Gateway 101g, instead of reverting to the default setting of "broadband."
DEV-14687	Cellular Airwall Gateways	Fixed an issue where the selected carrier was not showing up properly in Diag mode.
DEV-14686	Conductor	Fixed a few minor issues that could cause unsupported port group references in configuration data for an overlay DHCP and device port affinity.
DEV-14647	Cellular Airwall Gateways	Added a warning if you tried to select a carrier that wasn't compatible with the firmware installed on the Airwall Gateway 101g.
DEV-14636	Conductor	In people groups, if you add only blocking access windows, users can log in any time that access is not blocked. If you add both open and blocking access windows, then users can only log in during the open windows.
DEV-14629	Conductor	Clarified and fixed updating on Device Activity, Health Data, and Traffic Stats.
DEV-14608	Airwall Gateways	Fixed an issue that could prevent initialization of port groups with VLAN interfaces if the parent port was placed in a disabled port group.
DEV-14586	Conductor	Old tooltips no longer collect at the bottom of the screen
DEV-14577	Airwall Gateways	Fixed an issue where device activity wasn't reporting activity on bypass port groups with Routed only disabled.
DEV-14568	Airshell	Fixed issues with port group numbering when editing port groups in Airshell with 'conf network'.
DEV-14560	Airwall Gateways	Setting a 0.0.0.0/0 Bypass and blocking by hostname now correctly blocks the named destinations.
DEV-14557	Conductor, Airwall Gateways	Fixed an issue where some device discovery notifications were missed by Conductor.
DEV-14504	Conductor	Filtering alerts with a search term in the Alerts list now filters incoming alerts as well.
DEV-14429	OpenHIP	HIP is now more responsive to failures.
DEV-14427	Conductor	Fixed an issue where IPv6 DHCP settings sometimes showed IPv4 options after choosing Select one .
DEV-14335	Linux Airwall Servers	Fixed an issue that caused file handle leakage on Airwall Servers after running packet captures.
DEV-14264	MAP2-Client	You can now choose whether to replace or augment Airwall Gateway-configured Conductor URLs with those configured on the Conductor.
DEV-14233	Virtual Airwall Gateways	Amazon EC2 Airwall Gateways using ENA network drivers will now start with the second interface disabled instead of defaulting to an overlay port group.

ID	Applies to	Description
DEV-13951	Conductor	Conductor now provides an error message when attempting to pair with a Conductor that is already in Standby.
DEV-13763	Airwall Gateways	The Airwall Gateway 110 now detects the full 1GB of RAM rather than only 512MB.
DEV-11649	Airwall Gateways	Ping peer Airwalls now works for IPv6 peers on Linux-based platforms.

Known Issues

ID	Applies to	Description
New DEV-15302	macOS Airwall Agents	<p>The macOS Airwall Agent profile will not work correctly when restored to a new machine via Timemachine.</p> <p>Workaround -- Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one for that agent.</p>
DEV-15378 & DEV-15309	Airwall Gateways	<p>Unable to synchronize MAP after deleting port mirroring destination local device.</p> <p>Workaround – Add back the device that you just deleted. Then remove the Port Mirroring config before deleting the device.</p>
DEV-15370	Airwall Gateways	<p>Passive device discovery doesn't work on port groups that have Routed traffic only checked.</p>
DEV-15367	Conductor	<p>If you have two people groups with access windows, one giving a user access and another blocking access during the same time period, the user is allowed to complete user authentication when they should be blocked.</p> <p>Workaround – If possible, do not have allow and blocked access windows that overlap.</p>
DEV-15357	macOS Airwall Agents	<p>If you update the macOS Airwall Agent to a release later than v2.2.11 on macOS Mojave using a Conductor-based update package, it may not report the updated version to the Conductor.</p> <p>Workaround – Restart the agent or reapply the update.</p>
DEV-15356	Conductor	<p>Customer must "restart metadata cache" on conductor after attempting a replace.</p>
DEV-15305	Conductor	<p>Conductor does not validate the local device MAC address is a unicast address.</p>

ID	Applies to	Description
DEV-15219	MAP2-Client, OpenHIP	Airwall Gateways are not working on the Bell Mobility (Canada) cellular provider, due to the required use of a http/https proxy. (A major development effort would be required to support this.)
DEV-15031	Airwall Gateways	Remote syslog over TLS doesn't work when using keys stored in TPM
DEV-14957	iOS Airwall Agents	On iOS Airwall Agents, you must have Safari as your default browser to create a profile.
DEV-14835	Conductor	Airwall Gateway 150 serial numbers look like exponentiated numbers to Excel, so the column displaying the Serial number shows xxxEyyy instead of the full serial number.
DEV-14798	Conductor, Airwall Agents and Servers	Airwall Agents and Servers with negative policy will still be able to talk to each other via their LSI. The peer will also still show up in the UI.
DEV-14772	macOS Airwall Agents	If the macOS Airwall Agent is set to "off on boot" and the computer is rebooted, DNS may not be correctly set at startup. Workaround – Restart the agent to regain access to DNS. Stop the agent, if desired, to return to the DNS servers as given by DHCP.
DEV-14739	Airwall Gateways	If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved. Workaround – If you need both IPv4 and IPv6, set static IP addresses for both.
DEV-14736	Cellular Airwall Gateways	Cellular details may display as "unavailable" on the first boot after you update an Airwall Gateway. The cellular connections are not affected. Workaround – Reboot the Airwall Gateway again to correctly display the cellular details.
DEV-14726	Conductor	If you're viewing an Android Airwall Agent Ports page and the Airwall Agent changes how it's connected to the Conductor (for example, from WiFi to cellular), the display doesn't update correctly. Workaround – Refresh the page.
DEV-14715	macOS Airwall Agents	Big Sur ARM64 Macs are not supported in this release
DEV-14610	Conductor	After changing the Reporting traffic stats reporting time, the CPU graph will not display. Workaround – Refresh your browser page.

ID	Applies to	Description
DEV-14584	Cellular Airwall Gateways	<p>Hot-swapping the SIM on an Airwall Gateway 110 with firmware version 2.2.11 may not work.</p> <p>Workaround – Reboot the Airwall Gateway after installing a new SIM card.</p>
DEV-14570	Conductor	If you set an Airwall Agent owner to a user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 instead of a helpful error message.
DEV-14551	Conductor	The Android Airwall Agent lets you press the Edit Settings button on the Ports page; however, submitting any changes to the page results in an error message.
DEV-14509	Airwall Gateways	In Diagnostics, Ping peer Airwalls may return false negatives.
DEV-14426	Conductor, Airwall Gateways	Bypass destinations with a hostname do not show device activity in the Conductor.
DEV-14361	Airwall Gateways	The Build new tunnels if none exist option doesn't build tunnels to peer Airwall Edge Services with IPv6-only policy. This feature currently depends on having IPv4 policy between peer Airwall Edge Services.
DEV-14249	iOS Airwall Agents	<p>Check Secure Tunnels / Tunnel Status may show as unavailable on iOS.</p> <p>Workaround – You can determine tunnel status by checking packets sent or received.</p>
DEV-13970	Cloud-Alibaba, Conductor	<p>When you upgrade a Conductor on Alibaba Cloud, the Conductor system time gets out of sync.</p> <p>Workaround – To resync the time, go to Settings > Other settings > System time and date, select Edit Settings, then Update.</p>
DEV-13775	Cloud-Azure	The Conductor might rarely give a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed. If you get this error message, go to Azure portal and check the actual deployment result.
DEV-13760	Conductor	Device export/import does not export or import Bypass Devices.
DEV-13754	Android, Linux, and macOS Airwall Agents and Servers	The Conductor can falsely report that a macOS Airwall Agent is offline in some cases.

ID	Applies to	Description
DEV-13620	Conductor	In Airwall > Ports > Failover settings , the failover ping occurs only every "ping rate" + "ping timeout" seconds, somewhat unexpectedly.
DEV-13588	Conductor	Opening the Conductor on Internet Explorer 11 can be very slow for medium to large deployments. Workaround – Use the latest version of Chrome, Firefox, or Edge instead.
DEV-13544	Linux Airwall Servers	If no relay is configured, checking Relay probe information on the Linux Airwall Servers returns an error.
DEV-13531	Cloud	Automating creating Cloud HA Conductors only works with same cloud provider used for both active and standby. For example, AWS HA Active and AWS HA Standby. Workaround – You can manually set up different cloud providers as HA pair Conductors.
DEV-13474	Airwall Gateways	Configuring multiple overlay port groups with the same overlay IP subnet (same or different IP addresses) and then creating a local device equal to the entire subnet with port affinity set may not lead to the expected result.
DEV-13331	Cloud-Alibaba	Alibaba Cloud Conductor system time is incorrect. Workaround – Change the Conductor system time to browser time: In Conductor Settings , under System time , select Edit settings , select Set browser time , and then select Update .
DEV-13195	Conductor, Airwall Gateways	When you upgrade a Cellular Airwall Gateway-150 from 2.2.3 to 2.2.5, the cellular details all become "Unavailable." Workaround – Reboot and the details return.

ID	Applies to	Description
DEV-12852	Windows Airwall Agents and Servers	<p>Windows by default doesn't allow multiple 'active' interfaces. It prefers ethernet over cellular whenever possible.</p> <p>Workaround – Set Windows to keep multiple interfaces open by editing the fMinimizeConnections registry value:</p> <ol style="list-style-type: none"> 1. Hold the Windows Key and Press R. 2. In the run dialog, type regedit and click OK. 3. Navigate to the following path in Registry Editor: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\4 4. See if the GroupPolicy subkey exists. If not with, WcmSvc highlighted, right click on WcmSvc and Choose New > Key and name it GroupPolicy. 5. Right-click GroupPolicy and choose New > DWORD (32-bit) > Create value. 6. Name the value "fMinimizeConnections," and select OK. (The value should be 0, or false). Reboot and test.
DEV-11710	macOS Airwall Agents	<p>If you change the LSI prefix on the Conductor, the macOS Airwall Agent doesn't update the routes correctly.</p> <p>Workaround – Close and reopen the macOS Airwall Agent.</p>
DEV-10590	Cloud	The Conductor does not display an error when adding a route that would exceed the maximum number of allowed routes in the cloud provider.
DEV-10039	Airwall Gateways	An Airwall Gateway 150 can show "could not detect attached switch" intermittently.
DEV-9546	150 Airwall Gateways	The Airwall Gateway 150 serial connection has an intermittent issue when large amounts of data are sent over the console.
DEV-9429	Windows Airwall Agents and Servers	<p>Updating the Overlay Device IP address for a Windows Airwall Server in the Conductor doesn't update the first time.</p> <p>Workaround – Open and update the address a second time.</p>

Release Notes 2.2.10 Hotfix – Airwall Gateway HF-1

Release Date: Dec 16, 2020

This is a hotfix to release v2.2.10 for Airwall Gateways. See [Release Notes 2.2.10](#) on page 516 for more additions in version 2.2.10. Download HF-1 from [Hotfixes](#) on page 454. See also [Release Notes 2.2.10 Hotfix – Conductor HF-1](#) on page 514.



Note:

Also install Conductor HF-1, as it fixes some of these issues from the Conductor side. See [Release Notes 2.2.10 Hotfix – Conductor HF-1](#) on page 514.

What's New

IPv6 Support Added for Seamless Bypass

You can now use IPv6 with Seamless Bypass

See more:

- [Set up a secure IPv6 overlay](#) on page 316
- [Seamless Bypass](#) on page 329

Upgrade Considerations

Upgrade to this 2.2.10 hotfix if you were experiencing any of the following issues:

- An Airwall Gateway stops tunneling traffic after a reboot or a link fail-over.
- You want to access IPv6 bypass destinations.

Fixes

ID	Applies to	Description
DEV-14849	Airwall Gateway	Fixed a bug that could cause the root file system to fill up with log messages on some virtual platforms.
DEV-14817	Airwall Gateway	Fixed an issue that prevented using IPv6 with seamless bypass.
DEV-14815	Airwall Gateway	Fixed an issue that could cause Airwall Gateways to lose their policy configuration after reconnecting to the Conductor.
DEV-14814	Airwall Gateway	Include IPv6 policy-based routing rules or routing table in diagnostic report to help troubleshoot IPv6 connectivity issues.

Known Issues

See [Release Notes 2.2.10](#) on page 516 for known issues.

Release Notes 2.2.10 Hotfix – Conductor HF-1

Release Date: Dec 16, 2020

What's New

2.2.10 Conductor Hotfix HF-1

This is a hotfix to release v2.2.10 for the Conductor. See [Release Notes 2.2.10](#) on page 516 for more additions in version 2.2.10. Download HF-1 from [Hotfixes](#) on page 454.

**Note:**

Also install Airwall Gateway HF-1, as it fixes some of these issues from the Airwall Gateway side. See [Release Notes 2.2.10 Hotfix – Airwall Gateway HF-1](#) on page 513.

Upgrade Considerations

Upgrade to this 2.2.10 hotfix if you:

- Ran into issues where an Airwall Gateway stops tunneling traffic after a reboot or link fail-over.
- Want to include in the syslog Agent logon/logoff information.
- Need **Airwall Invitations** to not expire in a short time
- Use localized time that is in dd/mm/yy and not US mm/dd/yy and use invites.

Or you were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
DEV-14894	Conductor	The syslog now includes remote session (login via agent / server) creation, failed attempts, and termination.
DEV-14873	Conductor	Fixed an issue where the link to set your password for a new user that is provided by email expires very quickly. The expiration is now set to 2 weeks from the date of the invite.
		<p>Workarounds</p> <ul style="list-style-type: none"> – Go to the login page and reset your password to generate a new reset password token and then follow instructions in the email you receive. – Have your admin manually set the password. <p>Additional issue that was fixed was an issue where error messages (e.g. from passwords that do not meet the necessary criteria) were not being displayed on the reset password page.</p>
DEV-14870	Conductor	Fixed the OpenID Connect integration so that it works correctly with Azure AD platform.
DEV-14859	Airwall Gateway	Added a notification with the reason why a firmware update failed.
DEV-14846	Conductor	The expiration date in Airwall Invitations now displays in localized time formats.
DEV-14832	Conductor	Fixed an issue where revoking an Airwall Edge Service caused a deadlock and service restart on the Conductor.
DEV-14774	Conductor	Airwall Invitations created via the API did not include the activation code in the response.

ID	Applies to	Description
DEV-14765	Conductor	Overlay network dialog to manage devices and device groups now filters bypass destinations under their own heading.
DEV-14763	Conductor	Bulk deleting checked alerts was causing an issue with real time Conductor notifications.

Known Issues

See [Release Notes 2.2.10](#) on page 516 for known issues.

Release Notes 2.2.10

Release Date: Nov 18, 2020

What's New

Access Windows for authenticated users

Specify or restrict what days and times authenticated users can log in to access resources on your secure network using Access Windows.

See more: [Set Times Authenticated Users can Access the Secure Network](#) on page 78

Automatic Relay Rules

Enable all connections in an overlay network to use a group of relays. This provides a less-granular, but simple way to manage relay rules.

See more: [Set an Overlay to Automatically Manage Relay Rules](#) on page 82

Airwall Gateway Custom Certificates

By default, Airwall Gateways come with a Tempered factory-installed certificate. You can now add your own custom CA certificate to use for Conductor communication.

See more: [Add or Replace a Signed Certificate on an Airwall Gateway for Conductor Communication](#) on page 319

Bulk Configuration of Airwall Gateways

Configure certain settings in bulk for Airwall Gateways or Airwall Gateway groups.

See more: [Bulk Configuration of Airwall Edge Services](#) on page 314

Enable DNS for Seamless Bypass

You can now enable DNS to use fully-qualified domain names (FQDN) for bypass destinations.

See more:

- [Enable DNS lookup for bypass destinations](#) on page 336
- [Seamless Bypass](#) on page 329

Setup Wizards for configuring Conductors and Airwall Gateways

2.2.10 has added two wizards to help you in deploying an Airwall secure network. The Conductor Deployment Wizard walks you through setting up, licensing, and provisioning a new Conductor, and the new Airshell (`airsh`) command `setup-ui` walks you through the most common Airwall Gateway setup options.

See more:

- [Conductor Configuration Wizard Settings](#) on page 165
- [Configure an Airwall Gateway with the airsh Setup Wizard](#) on page 237

Airwall Status Indicators

There are new ways to see information and status on the Airwall Edge Services connecting to your Airwall secure network

See more: [See Airwall Edge Service Information and Status](#) on page 98

Cloud Improvements

This release includes improvements that make it easier to deploy cloud Conductors and Airwall Gateways, and includes support for AWS GovCloud (see below):

- **ENa and SR-IOV support** – You can now deploy instances with enhanced networking configuration enabled with either ENa or SR-IOV, and see which machine types support or require ENa. Note that machine types marked as ENa may deploy as SR-IOV.
- **Disk IO has been improved** – Cloud deployments now include NVMe (memory) disk options.
- **Cloud HA deployment has been automated** – Simplified deployment for HA, eliminating many of the places where misconfiguration could happen.
- **New Azure cloud image names** – Image names now reflect their use, making it easier to choose the correct image.
- **Additional information as images are created** – More details are included in the status pane as the Conductor creates cloud images.
- **Can now choose resource groups** – You can now choose a new or existing resource group when you create cloud Airwall Gateways and Conductors.

Note: If you choose an existing resource group, make sure no resource names in the existing resource group conflict with the new Airwall Gateway and Conductor deployment name that you are creating.

- **More information available in the Conductor** – New attributes are shown for cloud Airwall Gateways on the **Diagnostics** tab.

Preliminary IPv6 Support

If you have devices with IPv6 addresses, IPv6 is now supported for Airwall Gateways and Linux Airwall Servers. The control for source NAT is shared for both IPv4 and IPv6. Configurations sourcing NAT IPv4 but not IPv6 are not supported.

Airwall Gateways now support static IPv6 addresses for both the underlay and overlay (some cellular carriers may not support it). You also need to assign a static IPv6 address to the Airwall Gateway.

Since IPv6 only supports routed configurations, you need to assign an IPv6 overlay address to the Airwall Gateway to use IPv6 overlay. L2/subnet extensions are not supported.

See more: [Set up a secure IPv6 overlay](#) on page 316

AWS GovCloud Support

Cloud Conductors and Airwall Gateways can be now be deployed in AWS GovCloud. Follow the instructions for deploying in AWS:

- [Deploy a Conductor on Amazon Web Services \(AWS\)](#) on page 174
- [Set up Cloud Providers](#) on page 364
- [Deploy a cloud Airwall Server](#) on page 299

Exponential Backoff

Added exponential backoff to the Airwall Gateway to/from Conductor management connection to comply with Verizon data retry requirements. This change means it could take up to 3 minutes to reconnect after an extended outage. (*DEV-14648*)

Upgrade Considerations

Consider upgrading to 2.2.10 if:

<p>You want to use any of the following features:</p> <ul style="list-style-type: none"> • Access windows for authenticated users • Automatic relay rules • Custom certificates for Airwall Gateways • Bulk configuration of Airwall Gateways • Enabling DNS for bypass destinations • Setup wizards for Airwall Gateways or the Conductor • Improved Airwall Status • Cloud deployment improvements • IPv6 support • AWS GovCloud deployment 	<p>You were impacted by any issues discovered in prior releases, especially if you have any of the following:</p> <p>Ran into the issues where:</p> <ul style="list-style-type: none"> • Setting an Overlay default gateway breaks connected routes • Invites have incorrect links and configuration issues • Got errors on the Airwall Gateway 110g when running certain <code>airsh</code> commands <p>You want to:</p> <ul style="list-style-type: none"> • Access the Conductor firmware update server via a proxy • Disable individual devices in a bypass configuration • Allow network admins to manage new devices or agents • Use serial over IP on an Airwall Gateway 110e or 110g.
---	--

New and updated Airwall help content

In addition to help for new features, here are the changes to content published since our last release:

New Topics –

- [Troubleshoot Initial Airwall Gateway connections](#) on page 415

Updated –

- [Create an overlay network](#) on page 355
- [Update Airwall Gateway firmware](#) on page 108
- [Update firmware for a group of Airwall Edge Services](#) on page 110
- [Download Airwall Edge Services firmware updates](#) on page 108
- [Replace an Airwall Gateway](#) on page 111
- [Monitor Activity and Connections](#) on page 100
- [Log in and Configure the Conductor](#) on page 169
- [License and Provision a Conductor \(v2.2.8 and earlier\)](#) on page 160

- [Deploy a Physical Conductor](#) on page 168
- [Conductor and Airwall Edge Service PCI Compliance](#) on page 116
- [Set up Microsoft Azure as a cloud provider](#) on page 365

Fixes

ID	Applies to	Description
DEV-14703	OSX Airwall Agents	macOS Big Sur – Modified the OSX installer to correctly install on macOS Big Sur.
DEV-14675	Cellular Airwall Gateways	The Airwall 110g firmware now sets the DevInfo/Man and DevInfo/Mod OMA-DM strings when connected to Verizon.
DEV-14623	OpenHIP	v2.2.8 Mac Airwall Agents may form unusable tunnels with older 2.1.7 (and possible other versions) peer Airwall Edge Services, if traffic is being sent when the Airwall Agent is starting up.
DEV-14590	Conductor	Fixed an issue with JSON serialization of underlay and map IPs in the PCI Airwall reference.
DEV-14581	Airwall Gateways	Fixed an issue where when failover groups were configured to not use the Conductor as a ping destination and with the Conductor address using a hostname, the Airwall Edge Service is unable to connect to the Conductor by hostname.
DEV-14558	Airwall Gateways	Due to a bug in firmware versions 2.2.2 - 2.2.8, Airwalls using a TPM-backed keystore cannot update directly to firmware version 2.2.10. Should you run into this bug, you'll see the following message on the Reporting -> Health Data page of the Conductor: "firmware_verify: The currently selected keystore is not compatible with the target software version. Please factory reset the Airwall Gateway with the keystore=file argument to downgrade." To install firmware version 2.2.10 on a TPM-enabled Airwall Gateway, apply Airwall Gateway Hotfix-14558 first and then install 2.2.10 normally. See Hotfixes on page 454.
DEV-14521	Conductor	Fixed a health data setting for 2.2.8 Android and Windows Airwall Agents that may have had their health data inadvertently turned off.
DEV-14510	Airwall Gateways	Source UDP and TCP port are now randomized when passing through a bypass configuration with SNAT enabled. This change fixes a rare case where both the bypass gateway and another Airwall Gateway behind it are trying to communicate with the same peer (for example, a relay).
DEV-14506	Android and Windows Airwall Agents	Fixed an issue where modifying the reporting_interval for traffic stats via the Conductor would disable health data on the agents that supported it.
DEV-14461	Airwall Gateways	Fixed an issue where if overlay device NAT was configured on a port group with multiple ports, the overlay device NAT was incorrectly applied to traffic between the two ports in the same port group.
DEV-14447	Linux Airwall Servers	Fixed an issue where the support bundle for a Linux Airwall Server was missing attributes.

ID	Applies to	Description
DEV-14434	Airwall Gateways	IPv6 bypass is now functional for cellular underlay links.
DEV-14424	Conductor	Rate limited how often the bypass destinations traffic timestamp is updated to prevent negative performance impact on the Conductor.
DEV-14406	Conductor	Disabling traffic stats and health data monitors now works.
DEV-14394	Conductor	Fixed an issue that could cause revoked and re-activated Airwall Edge Services to fail to reconnect to the Conductor.
DEV-14389	Conductor	Fixed an issue where unmanaged or revoked Airwall Edge Service attributes could be updated using the API.
DEV-14359	Android Airwall Agents	Fixed an issue where switching underlays would cause the old underlay to be reported as unknown in the Traffic stats tab under reporting on the Conductor.
DEV-14356	Airwall Gateways	Fixed an issue where you could enable STP on port groups that use only a single port interface.
DEV-14312	Conductor	Fixed a broken download link in Linux Airwall Server setup.
DEV-14307	Airwall Gateways	Now allow Airwall Gateways and Linux Airwall ServerAirwall Servers to carry traffic within the LSI prefix (default to 1.0.0.0/8) across HIP tunnels, except for addresses that collide with peer Airwall Edge Service LSI addresses.
DEV-14291	Airwall Gateways	Fixed an issue that could cause a service crash on Airwall Edge Services when there was a network-related HA failover/fallback.
DEV-14278	Android Airwall Agents	Fixed an issue where replacing an Android Airwall Agent while the Android Airwall Agent service was running required the Airwall Agent to be restarted to get its new configuration and restore pings.
DEV-14266	Airshell	Fixed an issue preventing the 'diag-report' command from returning data under Airshell on the AW-110g. Diagnostic reports (system reports) take much longer to generate on cellular platforms.
DEV-14265	Airshell	Fixed Airshell 'status cell' command on the AW-110g, which sometimes repeatedly produced an error response.
DEV-14254	Conductor	Fixed an issue where Airwall Agents were showing up when creating a device discovery event monitor.
DEV-14251	Airwall Gateways	Fixed an issue introduced in Airwall Gateway HF-1 that could cause traffic to get blocked on Airwall Gateways with multiple overlay port groups.
DEV-14244	Azure Cloud Conductor	Fixed an issue where you were not able to select VNet when setting up a cloud Conductor.
DEV-14243	Airwall Gateways	Fixed an issue where broadcast and multicast received on an L2 bypass port group was consuming unnecessary bandwidth.
DEV-14228	Conductor	Fixed an issue where devices in smart device groups with tags may not have been removed correctly when the tags existed on both the devices and Airwalls or Airwall groups .

ID	Applies to	Description
DEV-14222	OpenHIP	Fixed an issue where DHCP configuration wasn't being updated.
DEV-14220	Conductor	Fixed an issue where you could not update an existing rule order and create a new device match rule with the old order of the existing rule.
DEV-14209	Android Airwall Agents	Fixed an issue where the Airwall Agent crashed the first time the user tried to start the service for a new profile.
DEV-14195	Conductor	Conductor Firmware downloader and OUI updater will now use the Conductor proxy settings.
DEV-14194	Airshell	Fixed an issue where the 'policy' command in Airshell returns an error under certain (larger, busier) deployments.
DEV-14191	Airwall Gateways	Fixed an issue that could cause traffic problems in deployments with multiple overlay port groups on the same broadcast domain.
DEV-14179	Conductor	Fixed an issue where the clock color indicating when a user last logged in was incorrect .
DEV-14172	Airwall Gateway 110g	Disabled IMS when using the Airwall Gateway 110g on T-Mobile.
DEV-14167	Windows Airwall Agents and Servers	Fixed an issue where the Conductor was showing Windows Airwall Agents had an update available when they already had that version installed. Note that you may still see updates available for x64 Windows if you have x32 firmware downloaded on the Conductor.
DEV-14166	Cellular Airwall Gateways	Fixed an issue when using customer-specific Verizon APNs on the Airwall Gateway 110g.
DEV-14159	Airwall Gateways	Fixed an issue where overlay traffic could flood out overlay ports.
DEV-14128	Conductor	The traffic stats monitor alert now more clearly indicates what is being measured, that is, kB/s, pkts/s
DEV-14123	Conductor	Notices on the login screen are now only displayed one time and disappear for your next visit to the page.
DEV-14119	Conductor	Fixed an issue where Airwall groups were not applying tags as the group was created.
DEV-14115	Conductor	Fixed an issue that could cause infrequent Conductor service issues resulting in all Airwall Edge Services needing to reconnect to the Conductor.
DEV-14113	Conductor	Fixed an issue where you could create policy to a bypass destination from a gateway's device even though the gateway has bypass disabled on its underlay.
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications for a device deleted any tags on it. This issue also was occurring when if you updated a device, device group, Airwall group, overlay network, or people group using the API.

ID	Applies to	Description
DEV-14100	Conductor	Fixed an issue where if you added a device directly to a device group in an Airwall invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable Airwall policies.
DEV-14095	Android Airwall Agents	Fixed an issue where the Overlay networks page was showing inaccurate ping counts.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API. IPs used for the map connection are now in the "map_ips" key in the API.
DEV-14070	Conductor	Fixed an issue where Airwall Edge Services coming online were not being included in Recent Activity.
DEV-14068	Android Airwall Agents	Fixed an issue where rotating the screen cleared the username and password when attempting to log in using User Auth.
DEV-14062	Conductor	Fixed a display issue when changing the pagination size on the monitors page.
DEV-14044	Android Airwall Agents	Fixed an issue where the ping status icon on the Overlay Networks/Edge Services page was always blue when pinging.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.
DEV-14013	Conductor	Standardized timestamps for Airwall Agents and Servers to display in the user's locale.
DEV-14009	Conductor	Fixed an issue where you couldn't remove static routes from a Conductor.
DEV-13984	Airwall Gateways	Fixed an issue where specifying the gateway on an overlay IP prevented creating the local subnet/connected route.
DEV-13978	Conductor	Fixed an issue where a device with an unknown OUI didn't update when the OUI list was updated.
DEV-13963	Linux Airwall Servers	Fixed an issue where HIP was restarting on the Centos7 Airwall Server.
DEV-13948	Cellular Airwall Gateways	Fixed an issue where sometimes the IMEI is listed as "unavailable" in Airshell and diagnostic mode when the affected Airwall Gateway does not have a sim card installed.
DEV-13946	Conductor	Fixed an issue where when you disabled an Airwall Agent or Server, it was not showing a disabled tag in the devices list.
DEV-13944	Conductor and Airwall Gateways	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.
DEV-13943	Conductor	Fixed an issue where the Tag actions did not list that devices would be impacted.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks in the network creation wizard.

ID	Applies to	Description
DEV-13935	API	Fixed an issue where network admins were unable to get the job status of Airwall Edge Service support jobs that they started in the API.
DEV-13930	Alibaba Cloud Conductor	<p>If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet.</p> <p>Workaround: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways.</p> <p>Workaround if you have already created an Alibaba Cloud Airwall Gateway:</p> <ol style="list-style-type: none"> 1. Apply this hotfix to your Conductor. 2. If you are not using an NTP for system time, on the Settings page, General setting tab, under System time, select Edit Settings, and then Under Update date and time, select Set browser time and then select Update. 3. For any cloud Alibaba Airwall Gateways, on the Cloud tab, Diagnostic subtab, click Refresh.
DEV-13926	OpenHIP	Fixed a rare packet allocation failure issue on the Airwall Gateway 100.
DEV-13916	Airwall Gateways	Fixed an issue where using DNSSRV records for Airwall Gateway provisioning caused the Conductor configuration to be lost.
DEV-13914	Conductor	Fixed an issue where if you used multiple serial over IP devices on the same Airwall Gateway (only supported on some profiles), you could create an invalid configuration when both devices are configured with the same IP but different ports.
DEV-13910	Conductor	You now receive a warning when creating a monitor on a device or Airwall group when some members of the group do not support the monitor. Previously, you only received such a warning for remote monitors (monitors run on the Airwall Edge Service).
DEV-13904	Google Cloud Conductor	Fixed an issue in the Google Cloud images for 2.2.8 Conductor and Airwall Gateways.
DEV-13903	Airwall Gateways	Airwall Gateway 110 models now can use the link failover monitor.

ID	Applies to	Description
DEV-13893	Conductor	Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, the Mac, Linux, or iOS platforms as of 2.2.8)
DEV-13860	Conductor	Fixed an issue where when creating a new device, the Port affinity drop-down menu showed the first overlay port group, but the value set was "Detect automatically."
DEV-13850	Conductor	Fixed an issue where network administrators couldn't manage an Airwall Edge Service from Recent events Dashboard notifications.
DEV-13844	Conductor	When replacing a high-availability paired Airwall Gateway, the Conductor now only lists Airwall Gateways that have an HA port configured.
DEV-13817	Airwall Gateways	Fixed an issue where the DHCP server on an Airwall Gateway Overlay Port Group was not restarting after changing the 'LSI prefix' on the Conductor.
DEV-13813	Airwall Gateways	Fixed an issue with the serial ports of the Airwall Gateway 110 where RS232 with hardware flow control (RTS/CTS), RS422 (full duplex) and RS485 (half duplex) were not functional. Airwall Gateway firmware version 2.2.10 and later supports all three serial port modes.
DEV-13768	Airwall Gateways	Fixed an issue where the source NAT setting on a bypass underlay port group was not updating the setting.
DEV-13765	Airwall Gateways	Fixed an issue where bypass underlay port groups with source NAT enabled and routed mode disabled did not allow incoming connections from the underlay.
DEV-13759	Airwall Gateways	Fixed an issue where the Detect Devices button sometimes incorrectly included devices attached to other port groups or peer Airwall Gateways if policy permitted traffic from an Overlay IP to those destinations.
DEV-13755	Cellular Airwall Gateways	Disabled LWM2M reporting on the Airwall Gateway 110g when using the AT&T carrier configuration. AT&T ODIS requirements are met by using a product specific IMEI TAC.
DEV-13748	Conductor	Fixed an issue where if you disabled overlay MTU, the change was not immediately sent to Airwall Gateways.
DEV-13744	Conductor	Fixed an issue where the Airwall group dialog allowed you to attempt to modify it even if you didn't have permissions.
DEV-13689	Conductor	Overlays, Devices, Airwalls, and People pages now have a consistent scheme for button and filter placement, with actions on the left and filters on the right.
DEV-13682	Airshell	Fixed an issue where multiple MAP URIs were not correctly displayed within Airshell ('status conductor', 'conductor status', and 'conductor set').
DEV-13664	Conductor	Email colors have been adjusted to be more legible in more email applications.

ID	Applies to	Description
DEV-13630	Cellular Airwall Gateways	Fixed a problem related to signal strength reporting from Airwall Gateways with a Quectel modem connected to a 3G network.
DEV-13621	Airwall Gateways	Improved the timing of link failure-related actions (like reboot or cellular session recycling) to reflect the configured timeouts more accurately.
DEV-13505	OpenHIP	Fixed high CPU usage by hipd thread.
DEV-13332	Cellular Airwall Gateways	Updated the Quectel EC25-AF firmware revision to EC25AFFDR07A09M4G_01.004.01.004, to address some AT&T related connection issues.
DEV-13297	Airwall Gateways	Fixed an issue where when an Airwall Gateway with seamless bypass is configured as layer 2 "bump in the wire," traffic from the protected device to remote protected devices on different subnets was not working as expected.
DEV-13275	Airwall Gateways	Fixed an issue where a misconfigured local device was corrupting the ARP cache entries for peer Airwall Gateways.
DEV-13272	Airwall Gateways	Improved the reliability of firmware updates in very low bandwidth situations.
DEV-13109	Airwall Gateways	Fixed Check secure tunnels diagnostic function: relays and relay clients are no longer included in the list.
DEV-10936	Airwall Gateways	You no longer need to cable HA Airwall Gateways directly, and should no longer see situations where both Airwall Gateways are active.
DEV-6147	Conductor	Fixed an issue where the placeholder text for an Airwall invitation "Generated Airwall name" was incorrect.
DEV-3342	Conductor	Fixed an issue where the firewall settings become unresponsive when editing Airwall Gateway settings.

Known Issues

ID	Applies to	Description
New DEV-15302	macOS Airwall Agents	The macOS Airwall Agent profile will not work correctly when restored to a new machine via Timemachine. Workaround -- Create a new profile on the Airwall Agent, and then on the Conductor, replace the old profile with the new one for that agent.
DEV-15039	Linux Airwall Servers	There is a small memory leak in the Airwall Linux Agent Server that might require a restart over the course of a month.
DEV-14981	Linux Airwall Servers	The Linux Airwall Server crashes when trying to ping peer Airwall Edge Services from the Conductor, and the server has around 15+ peers.

ID	Applies to	Description
DEV-14818	Airwall Gateways, Open HIP	<p>DNS-based Bypass opens up a possible security hole by allowing dynamic policy creations based on results of name lookup over the Internet. Combined with disabling Source NAT (SNAT), this leaves the Overlay open to attack from a sufficiently-technical attacker.</p>
		<p>Workaround – Enable SNAT on the Underlay when using DNS-based bypass destinations to prevent potential inbound access from arbitrary sources.</p>
DEV-14772	OSX Airwall Agents	<p>If the Airwall Agent is set to "off on boot" and the mac is rebooted, DNS may not be correctly set at startup.</p>
		<p>Workaround – Restart the agent to regain access to DNS. Stop the agent, if desired, to return to the DNS servers as given by DHCP.</p>
DEV-14767	AWS Cloud Conductor	<p>ENA required instance types won't be available in us-gov-east-1 region for GovCloud customers, and ap-east-1 & eu-north-1 regions for commercial cloud customers. ENA supported and unsupported instance types still work with these new regions.</p>
DEV-14743	Conductor	<p>The Airwall Gateway setting for DHCPv6 uses DHCPv4.</p>
DEV-14739	Airwall Gateways	<p>If you set IPv4 to DHCPv4 and set a static IP address for IPv6, the setting that you set second doesn't get saved.</p>
		<p>Workaround – If you need both IPv4 and IPv6, set static IP addresses for both.</p>
DEV-14736	Cellular Airwall Gateway 150s	<p>Cellular details may display as "unavailable" on the first boot after upgrade. Cellular connections are not affected.</p>
		<p>Workaround – Reboot the Airwall Gateway a 2nd time.</p>
DEV-14692	Airshell	<p>In the new Airshell 'conf network' menu system, when editing a port group, it is possible to enter unsupported or duplicate interfaces, or interfaces already in use by another port group.</p>
		<p>Workaround – Check the 'status network' output to check for duplicates to avoid unsupported or conflicting configurations.</p>
DEV-14688	Cellular Airwall Gateways	<p>After factory resetting a Verizon 101g, you must change the APN to 'vzwinternet' in diagnostic mode.</p>
DEV-14636	Conductor	<p>When adding Access windows to a people group, if you add a blocked window, you also need to add an Access window for the times you do want to give access. Otherwise users will always be blocked.</p>

ID	Applies to	Description
DEV-14610	Conductor	<p>After changing the Reporting traffic stats reporting time, the CPU graph will not display.</p> <p>Workaround – Refresh your browser.</p>
DEV-14608	Airwall Gateways	<p>If the parent port of a VLAN-tagged sub-port is placed in a disabled port group, the VLAN-tagged child-port will not be initialized correctly in all cases.</p> <p>Workaround – To work around this issue, do not place parent-ports that have VLAN sub-ports in a disabled port group. Instead, remove unneeded parent-ports from all port groups. This issue will be fixed in a future firmware revision.</p>
DEV-14606	Airwall Gateways	<p>When attempting to replace a HA member with a new Airwall Gateway, the Conductor allows you to select an Airwall Gateway that does not have an Overlay or HA port configured.</p> <p>Workaround – Make sure the Airwall Gateway you select has a workable HA port configuration.</p>
DEV-14595	Cellular Airwall Gateways	<p>When an Airwall Gateway 110g is started without a SIM card installed and Verizon selected as the carrier, the cellular modem will restart every 2 minutes until a SIM card is installed.</p>
DEV-14584	Cellular Airwall Gateways	<p>SIM hot-swap functionality is not guaranteed on firmware version 2.2.10 with the Airwall Gateway 110. Please reboot the Airwall Gateway after installing a new SIM card.</p>
DEV-14577	Airwall Gateways	<p>Device activity doesn't report activity on bypass port groups with routed only disabled.</p>
DEV-14570	Conductor	<p>If an Airwall Agent owner is set as any user (LDAP, local, or OIDC) and someone attempts to user authenticate with a different OIDC user, they will not be able to authenticate (which is the correct behavior), but they see a 500 error message instead of a helpful error message.</p>
DEV-14564	Conductor	<p>The following log messages can be safely ignored: [ERROR] error parsing message: msg= [ERROR] JsonRpcDispatcher: received unknown method: method= msg=</p>
DEV-14560	Airwall Gateways	<p>Assigning block policies to bypass destinations has no effect.</p> <p>Workaround – Create a bypass destination using the resolved IP address of the hostname and create blocking policy for it.</p>
DEV-14549	Android Airwall Agent	<p>Cellular details are not currently available on the Ports tab for Android Airwall Agents.</p>

ID	Applies to	Description
DEV-14518	Android Airwall Agent	<p>The Ports tab is now available for Android Airwall Agents with the following drawbacks:</p> <ul style="list-style-type: none"> • The cellular interface data is not available. • You cannot change anything on the Agent Ports tab.
DEV-14509	Airwall Gateways	<p>Diagnostics: Ping peer Airwall Gateways may return false negatives</p>
DEV-14504	Conductor	<p>Filtering alerts by name always includes new alerts, even if they don't match the filter keyword.</p>
DEV-14483	Airwall Gateways	<p>When you configure device NAT for devices on multi-port port groups, NAT is applied to the initial flow of intra-port group packets from those devices. Subsequent conversations will correctly omit the NAT.</p>
DEV-14467	Airwall Gateways	<p>Connecting an access port interface and a VLAN-tagged port interface within the same Airwall Gateway port group to an STP-enabled Cisco switch will trigger a Cisco port disable.</p> <p>Workaround – Set “no spanning-tree VLAN <#>” on the Cisco switch’s affected VLANs to prevent the port shutdown.</p>
DEV-14427	Conductor	<p>IPv6 DHCP settings sometimes show IPv4 options after choosing the 'Select one...' option.</p>
DEV-14426	Conductor, Airwall Gateways	<p>Bypass destinations with a hostname do not show device activity in the user interface.</p>
DEV-14361	Airwall Gateways	<p>The Build new tunnels if none exist setting doesn't trigger building tunnels on peer Airwall Edge Services with IPv6-only policy.</p>
DEV-14336	AWS Cloud Conductor	<p>If you choose an ENA machine type when creating a cloud Conductor on Amazon Web Services, you cannot downgrade or change it back to a non-ENA type. However, for a cloud Airwall Gateway, if you choose an ENA machine type, you can downgrade it if you first change it to a non-ENA machine type in Amazon Web Services.</p>
DEV-14308	OpenHIP	<p>Initial packets may be dropped while building a new tunnel to a new peer Airwall.</p>
DEV-14249	iOS Airwall Agents	<p>Check Secure Tunnels or Tunnel Status may be unavailable on iOS.</p> <p>Workaround – You can determine Tunnel status by checking packets sent/received.</p>

ID	Applies to	Description
DEV-14233	Virtual Airwall Gateways	Amazon EC2 Airwall Gateways using ENA network drivers will start with the second interface disabled instead of defaulting to an overlay port group.
DEV-14218	Airwall Gateways	NAT broadcast applies to traffic between ports within a single port group. Use an external switch if you need to connect multiple devices to a single port group and use the NAT broadcast feature and require IP broadcast un-NATed between those local devices.
DEV-14210	Conductor	Currently, when you set Source NAT, it configures it for both IPv4 and IPv6.
DEV-14208	Airwall Gateways	Bypass port groups do not currently support IPv6.
DEV-13970	Alibaba Cloud Conductor	When you upgrade a Conductor on Alibaba Cloud, the Conductor system time gets out of sync. Workaround – Go to Settings > Other settings > System time and date , click Edit Settings , then Update to resync.
DEV-13880	Diagnostic mode on Airwall Gateways	EAP-TLS does not work with current or previous WiFi Airwall Gateways (75w), so is now disabled. This setting will be reenabled once this feature is fixed.
DEV-13775	Azure Cloud Conductor	Conductor might rarely give "Net::ReadTimeout" error when user tries to deploy an Azure Airwall Gateway 300v or server. This doesn't indicate that the deployment has failed. If you get this error message, go to the Azure portal and check the actual deployment result.
DEV-13753	Azure Cloud Conductor	During cloud Airwall Gateway deployment, you can now choose an existing resource group, as long as you make sure the name of the Airwall Gateway deployment does not conflict with any resources in the existing resource group.
DEV-13271	Airwall Gateways	The Airwall Gateway 110 has CPU frequency scaling enabled, which allows it to save power under low load conditions. This results in high load average / CPU usage figures in Conductor when the Airwall Gateway 110 CPU is in its lowest power state. Future releases may improve CPU utilization.
DEV-12852	Windows Airwall Agents and Servers	The Windows Airwall Agent may not connect when multiple interfaces are active This issue can be caused by a Windows default that doesn't allow multiple simultaneous active network interfaces, and prefers ethernet over cellular or WiFi. It can be bypassed by editing a registry value. See the troubleshooting steps in I'm having trouble connecting on page 31.

ID	Applies to	Description
DEV-8824	Android Airwall Agents	The implicit SNAT for Airwall Agents without an Overlay IP is not applied from a pre 2.2.10 Android Airwall Agent to a 2.2.10 Airwall Gateway with SNAT disabled: please upgrade the Android Airwall Agent to 2.2.10 or later.

Release Notes 2.2.8 Hotfix – Conductor HF-5

Release Date: Dec 18, 2020

This is a hotfix to release v2.2.8 for Conductors. See [Release Notes 2.2.8](#) on page 537 for more additions in version 2.2.8. Download HF-5 from [Hotfixes](#) on page 454.

2.2.8 Conductor Hotfix HF-5 includes and replaces Conductor Hotfixes HF-1 through HF-4. Once installed, it will show all hotfixes (HF-1, HF-2, HF-3, HF-4, and HF-5) as installed.

What's New

This hotfix is a replacement for Conductor HF-4 that fixes **Airwall Invitations** that were expiring too quickly.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you were experiencing any of the following issues:

- Need **Airwall Invitations** to have a long expiration date.

Or if you were impacted by any of the other issues fixed in this or earlier hotfixes.

Fixes

ID	Applies to	Description
DEV-14901,	Conductor	Fixed an issue where the link to set your password for a new user that is provided by email expires very quickly. The expiration is now set to 2 weeks from the date of the invite.
DEV-14873		
Workarounds		
<ul style="list-style-type: none"> – Go to the login page and reset your password to generate a new reset password token and then follow instructions in the email you receive. – Have your admin manually set the password. <p>Also fixed an issue where error messages (e.g. from passwords that do not meet the necessary criteria) were not being displayed on the reset password page.</p>		
Includes HF-4 Fixes:		

ID	Applies to	Description
DEV-14424	Conductor	Rate limit how often a bypass destinations traffic timestamp will be updated to prevent negative performance impact on the Conductor.
DEV-14332	Conductor	Fixed an issue where if you deleted a tag owner, the UI wouldn't show any tags on the page that would be displayed below it.
Includes HF-3		
Fixes:		
DEV-14167	Windows Airwall Agent or Server	Fixed an issue where the Conductor was showing Windows Airwall Agents had an update available when they already had that version installed. Note that you may still see updates available for x64 Windows if you have x32 firmware downloaded on the Conductor.
Includes		
Conductor HF-2		
Fixes:		
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications of a device would delete any tags on it. Updating a device, device group, Airwall group, overlay network, or people group via the API would delete any tags on the updated object.
DEV-14080	Conductor	Fixed an issue where when adding a device directly to a device group in an Airwall Invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable policies.
DEV-14077	Conductor	Fixed an issue where the dashboard number for upgradeable Airwalls was including Airwalls that could apply an earlier version.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API.
DEV-14070	Conductor	Fixed an issue where Airwall Gateways coming online was not being included in an overlay network's Recent Activity.
DEV-14059	Conductor	Fixed an issue where you could apply HF-1 multiple times.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.
DEV-14009	Conductor	Fixed an issue where you sometimes couldn't remove static routes from an HA pair.
DEV-13944	Conductor, Airwall Gateway	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.
Includes		
Conductor HF-1		
Fixes:		

ID	Applies to	Description
DEV-13943	Conductor	Fixed an issue in the Tag Actions menu where devices with the tag were not included in the list of items that would be impacted by the action.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks.
DEV-13930	Cloud-Alibaba, Conductor	If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet. Workaround: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways. Workaround if you have already created an Alibaba Cloud Airwall Gateway:
		<ol style="list-style-type: none"> 1. Apply this hotfix to your Conductor. 2. If you are not using an NTP for system time, on the Settings page, General setting tab, under System time, select Edit Settings, and then Under Update date and time, select Set browser time and then select Update. 3. For any cloud Alibaba Airwall Gateways, on the Cloud tab, Diagnostic subtab, click Refresh.
DEV-13912	Conductor	Fixed an issue where secure tunnel status was not accurately reporting tunnel status for HA-paired Airwall Gateway's.
DEV-13904	Cloud-Google, Conductor	To deploy a 2.2.8 Google Cloud 300v Airwall Gateway from the Conductor, apply this hotfix.
DEV-13893	Conductor	Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, you now cannot select the Mac, Linux, or iOS platforms)
DEV-13888	Conductor	Fixed an issue where when you attempted to manage items from a New Airwall Online notification on the new Dashboard, it could be lost if another notice is received.
DEV-13870	Conductor	Fixed an issue where bandwidth would be reported multiple times, resulting in dashboard graphs reporting much higher throughput than the actual throughput.
DEV-13860	Conductor	Fixed an issue where when you were creating a new device, the Port affinity menu showed the first overlay port group, even though the value was set to Detect automatically .

Known Issues

See [Release Notes 2.2.8](#) on page 537 for known issues.

Release Notes 2.2.8 Hotfix – Airwall Gateway HF-3

Release Date: Oct 19, 2020

This is a hotfix to release v2.2.8 for Airwall Gateways. See [Release Notes 2.2.8](#) on page 537 for more additions in version 2.2.8. Download HF-3 from [Hotfixes](#) on page 454. See also [Release Notes 2.2.8 Hotfix – Airwall Gateway Hotfix-13955](#) on page 537.

2.2.8 Airwall Gateway Hotfix HF-3 includes and replaces Airwall Gateway Hotfixes HF-1 and HF-2. Once installed, it will show all hotfixes (HF-1, HF-2, and HF-3) as installed.



Note:

Also install Conductor HF-4, as it fixes some of these issues from the Conductor side. See [Release Notes 2.2.8 Hotfix – Conductor HF-4](#) on page 534.

What's New

This hotfix is a replacement for Airwall Gateway HF-2 that fixes a bug in the HA failover logic causing invalid HA state information to be displayed in the Conductor when the failover was triggered by network availability. The hotfix also fixes an issue that could cause excessive device activity event reporting on bypass ports with large device network objects as well as a problem when using device NAT with bridged overlay port groups.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you were experiencing any of the following issues:

- Conductor displaying an Invalid HA state for Airwall Gateways
- Excessive disk utilization on the Conductor and/or high network traffic between Airwall Gateways configured with a bypass port group and the Conductor
- Ping devices failures
- Airwall Gateways needing to reconnect to the Conductor
- Airwall Gateways failing a policy check on some overlay networks.

Or if you were impacted by any of the other issues fixed in this or earlier hotfixes.

Fixes

ID	Applies to	Description
Airwall Gateway HF-3:		
DEV-14452	Airwall Gateway	Rate-limited device activity events for network objects.
DEV-14451	Airwall Gateway	Fixed an HA issue after rebooting an Airwall Gateway
DEV-14449	Airwall Gateway	Fixed an issue where the overlay NAT was being applied to traffic between ports in an Overlay port group.
Includes Airwall Gateway HF-2:		
DEV-14247	Airwall Gateway	Fixed a bug that was introduced in Airwall Gateway Hotfix rollup-1 that could cause traffic to get blocked on Airwall Gateways with multiple overlay port groups.

ID	Applies to	Description
DEV-14190	Airwall Gateway	Fixed an issue that could cause traffic problems in deployments with multiple overlay port groups on the same broadcast domain.
DEV-14162	Airwall Gateway	Fixed an issue in Conductor HF-2 that was causing the "Ping devices" feature to fail for devices with plain IP addresses.
DEV-14115	Conductor	Fixed an issue that could cause infrequent Conductor service issues resulting in all Airwall Gateways needing to reconnect to the Conductor.
DEV-14067	Conductor, Airwall Gateway	Fixed an issue on 2.2.8 Airwall Edge Services that could cause false negatives in the policy check for some overlay network configurations.
DEV-13981	Airwall Gateway	Fixed an issue where setting an overlay default gateway prevented creating both the connected (local subnet) and default routes.
DEV-13974	OpenHIP	Fixed performance regression on multi-core platforms.
DEV-13926	OpenHIP	Fixed a rare packet allocation failure issue on Airwall Gateway-100.
DEV-13903	Airwall Gateway	Airwall Gateway-110 models now can use the link failover monitor.
DEV-13843	Airwall Gateway	Added firewall connection states to the diagnostic report.
DEV-13275	Airwall Gateway	Fixed an issue where a misconfigured local device was corrupting the ARP cache entries for peer Airwall Gateways.

Known Issues

See [Release Notes 2.2.8](#) on page 537 for known issues.

Release Notes 2.2.8 Hotfix – Conductor HF-4

Release Date: Oct 19, 2020

What's New

2.2.8 Conductor Hotfix HF-4

This is a hotfix to release v2.2.8 for the Conductor. This hotfix rolls up the previous Conductor hotfixes HF-1 through 3, so you only need to install HF-4. See [Release Notes 2.2.8](#) on page 537 for more additions in version 2.2.8. Download HF-4 from [Hotfixes](#) on page 454.



Note: Also install Airwall Gateway HF-3, as it fixes some of these issues from the Airwall Gateway side. See [Release Notes 2.2.8 Hotfix – Airwall Gateway HF-3](#) on page 533.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you have a bypass destination configured and are experiencing Conductor performance issues, or were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
HF-4 Fixes:		
DEV-14424	Conductor	Rate limit how often a bypass destinations traffic timestamp will be updated to prevent negative performance impact on the Conductor.
DEV-14332	Conductor	Fixed an issue where if you deleted a tag owner, the UI wouldn't show any tags on the page that would be displayed below it.
Includes HF-3		
Fixes:		
DEV-14167	Windows Airwall Agent or Server	Fixed an issue where the Conductor was showing Windows Airwall Agents had an update available when they already had that version installed. Note that you may still see updates available for x64 Windows if you have x32 firmware downloaded on the Conductor.
Includes Conductor HF-2		
Fixes:		
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications of a device would delete any tags on it. Updating a device, device group, Airwall group, overlay network, or people group via the API would delete any tags on the updated object.
DEV-14080	Conductor	Fixed an issue where when adding a device directly to a device group in an Airwall Invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable policies.
DEV-14077	Conductor	Fixed an issue where the dashboard number for upgradeable Airwalls was including Airwalls that could apply an earlier version.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API.
DEV-14070	Conductor	Fixed an issue where Airwall Gateways coming online was not being included in an overlay network's Recent Activity.
DEV-14059	Conductor	Fixed an issue where you could apply HF-1 multiple times.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.
DEV-14009	Conductor	Fixed an issue where you sometimes couldn't remove static routes from an HA pair.
DEV-13944	Conductor, Airwall Gateway	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.
Includes Conductor HF-1		
Fixes:		

ID	Applies to	Description
DEV-13943	Conductor	Fixed an issue in the Tag Actions menu where devices with the tag were not included in the list of items that would be impacted by the action.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks.
DEV-13930	Cloud-Alibaba, Conductor	If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet. Workaround: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways. Workaround if you have already created an Alibaba Cloud Airwall Gateway:
		<ol style="list-style-type: none"> 1. Apply this hotfix to your Conductor. 2. If you are not using an NTP for system time, on the Settings page, General setting tab, under System time, select Edit Settings, and then Under Update date and time, select Set browser time and then select Update. 3. For any cloud Alibaba Airwall Gateways, on the Cloud tab, Diagnostic subtab, click Refresh.
DEV-13912	Conductor	Fixed an issue where secure tunnel status was not accurately reporting tunnel status for HA-paired Airwall Gateway's.
DEV-13904	Cloud-Google, Conductor	To deploy a 2.2.8 Google Cloud 300v Airwall Gateway from the Conductor, apply this hotfix.
DEV-13893	Conductor	Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, you now cannot select the Mac, Linux, or iOS platforms)
DEV-13888	Conductor	Fixed an issue where when you attempted to manage items from a New Airwall Online notification on the new Dashboard, it could be lost if another notice is received.
DEV-13870	Conductor	Fixed an issue where bandwidth would be reported multiple times, resulting in dashboard graphs reporting much higher throughput than the actual throughput.
DEV-13860	Conductor	Fixed an issue where when you were creating a new device, the Port affinity menu showed the first overlay port group, even though the value was set to Detect automatically .

Known Issues

See [Release Notes 2.2.8](#) on page 537 for known issues.

Release Notes 2.2.8 Hotfix – Airwall Gateway Hotfix-13955

Release Date: Aug 4, 2020

What's New

2.2.8 Airwall Gateway Hotfix

This is a hotfix to release v2.2.8 for Airwall Gateways. See the [Release Notes 2.2.8](#) on page 537 for more additions in version 2.2.8. Download Hotfix-13955 from [Hotfixes](#) on page 454.

Upgrade Considerations

If you use DNSSRV to set the Conductor address on your Airwall Gateways, we recommend that you install this hotfix before upgrading them to 2.2.8 .

Fixes

ID	Applies to	Description
DEV-13916		<p>Fixed the use of DNS SRV records for Airwall Gateway provisioning. Apply HF-13955 before upgrading Airwall Gateways to firmware version 2.2.8 or after provisioning new 2.2.8 Airwall Gateways via a DNS SRV record.</p> <p>You can then install 2.2.8 on the Airwall Gateways.</p> <p>If you have already installed 2.2.8 on Airwall Gateways and are experiencing this issue, please contact support@tempered.io for assistance, or you can manually configure the Conductor address in each Airwall Gateway using airsh or Diagnostic mode.</p>

Known Issues

See [Release Notes 2.2.8](#) on page 537 for known issues.

Release Notes 2.2.8

Release Date: Jul 17, 2020

What's New



Note: These release notes were updated Jul 31, 2020 to include the release of the v2.2.8 Windows Airwall Agents and Servers, and Sep 9, 2020, with an update for the all Airwall Agents and Servers. New versions are in the [Latest firmware and software](#) on page 431.

New Airwall Gateway Hardware – the Airwall-110

The Airwall-110 Series is a major upgrade for the 100-Series, with higher performance and global cellular connectivity – all in a smaller form factor that maximizes the v2.2.8 improvements. The Airwall-110 has more (4x) bandwidth performance and two serial ports, runs all Snort intrusion detection monitors, handles up to 6 HD

video streams, and has more storage and memory (so it has higher capacity, quality, and scalability for production environments).

See more: [Airwall Gateway 110 Series](#) on page 122

New cellular modem support

Version 2.2.8 supports the upcoming North America and Global cellular expansion trays for our Airwall-150 appliance. These LTE Category 4 expansion modules come in two variants supporting North America and Rest of World. These expansion trays allow you to connect your Airwall 150 to more cellular carriers in more countries including the United States, Canada, Australia, New Zealand, Japan, the European Union, and other countries recognizing CE RED certificates.

Conductor Dashboard and Usability Improvements

The Conductor Dashboard has been improved to give you a broader look into the status of your Airwall secure network. New features include:

- Ability to pin pages you visit frequently
- See how many Airwall Edge Services are online, and how many authenticated users are logged in.
- Easily manage new provisioning requests
- See when new firmware and software is available, and easily update your network.
- Improved user onboarding workflow (see Improved User Management below)

See more:

- [The Conductor Dashboard](#) on page 32
- [Create or Manage Dashboard Messages](#) on page 39
- [Conductor Icon Reference](#) on page 36
- [Monitor Connections to your Airwall secure network](#) on page 104
- [Download Airwall Edge Services firmware updates](#) on page 108
- [Update firmware for a group of Airwall Edge Services](#) on page 110

Improved User Management and Remote Access User Features

Remote access user management has been expanded to scale for large organizations, with the Conductor doing most of the work that admins used to have to do to invite, onboard (especially installing and activating the Airwall Agents), orchestrate, and authenticate remote access users. Onboarded users can see what they can access through the overlay networks in Conductor, eliminating frequent support calls to Conductor admins for help getting server IP addresses.

See more:

Conductor Admin Topics

- [Connect People's Devices to your Airwall secure network](#) on page 54
- [Connect People as Remote Access Users](#) on page 61
- [Connect People's Devices with Activation Codes](#) on page 63
- [Set up a People Group](#) on page 74
- [Manage Versions of Airwall Agents and Servers](#) on page 106
- [Provision Airwall Gateways using Activation Codes](#) on page 161
- [Walkthrough - Onboard people to your Airwall secure network with User Authentication](#) on page 71

End user topics

- [Change my Conductor password](#) on page 30
- [I have an Activation Code](#) on page 14
- [I want to request to connect](#) on page 17
- [I have a "Finish Setting up my account" email](#) on page 14
- [Create or Edit Airwall Agent or Server Profiles](#) on page 29

- [I'm having trouble connecting](#) on page 31

Enhanced Monitoring

You can now set monitor thresholds on health data and traffic stats to detect potential problems before they occur. We have redline stats for performance metrics of the Airwall Gateway, and for volumetric traffic stats.

Seamless Bypass (split tunnel)

Seamless bypass enables you to deploy without knowing all of the hosts to allow in an overlay policy. Seamless bypass replaces the need to create policy exceptions, and reduces the complexity, extra hardware, extra cabling, and reliance on configuration of your underlay infrastructure.

See more: [Seamless Bypass](#) on page 329

Alibaba Cloud Conductor and Airwall Gateways

You can now use Alibaba Cloud to deploy cloud Conductors and Airwall Gateways, and seamlessly connect cloud Conductors and Airwall Gateways with each other, as well as virtual and on-premises or physical environments. You can deploy an Airwall secure network on all of the major cloud providers.

See more:

- [Deploy a Conductor on Alibaba Cloud](#) on page 171
- [Alibaba Cloud – Set up an Airwall Gateway](#) on page 268

Routed Port Group Improvements

The ability to configure port groups can give you up to a 30% performance increase for common deployment cases using a single interface in the overlay port group (for example, cloud gateways, virtual gateways, and optionally on physical gateways). It is simpler to deploy and avoids multicast/broadcast chatter over the tunnel.

See more:

- [Set up Port Groups on an Airwall Gateway](#) on page 321
- [Set up an Underlay Port Group](#) on page 324
- [Set up Overlay Port Groups](#) on page 321

Custom signed Certificate Improvements

You can replace a signed certificate on the Conductor with the old certificate remaining active until the new certificate is activated.

See more: [Add or Replace a Signed Certificate for the Conductor UI](#) on page 201

Easier Deployment of High Availability Cloud Conductors

The Airwall Solution has automated the process of creating high availability Conductors in the cloud across different providers. You can now back up your Conductor and easily create an HA standby in the cloud using the Conductor's automated process and be guaranteed a successful cloud HA deployment.

See more: [Automatically Create an Standby HA Conductor in the Cloud](#) on page 228

Remote Airshell Access into Airwall Gateways

You can securely log in to the overlay IP address of an Airwall Gateway with key-based SSH, and run Airshell (airsh) commands remotely. Airsh has been enhanced to perform many of the functions of diagnostic mode. Remote access can help avoid in-person visits to perform diagnostics and troubleshooting. Status and statistics are available using airsh, which includes tab-completion and inline help.

See more:

- Set up Remote Access to Airshell on page 310
- Access an Airwall Gateway Remotely on page 311

Port configuration replication

You can now replicate the port configuration between two Airwall Gateways when setting up an Airwall Gateway HA pairing, or when replacing an Airwall Gateway.

See more:

- Configure High Availability Airwall Gateways (v2.2.8 and later) on page 337
- Replace an Airwall Gateway on page 111

Device Manufacturer (MAC address OUI) is now displayed

The **Devices** list now shows the manufacturer's name determined from the MAC address OUI (organizationally unique identifier), where available, in the **OUI** column. You can also now update the OUI list as needed.

See more:

- Update the MAC address (OUI) (Manufacturer) List on page 413
- See MAC address OUI (Manufacturer) Information for Devices on page 97
- Search for or Sort Devices by MAC Address OUI (Manufacturer) Name on page 97

Manage Airwall Agents through an MDM

Some MDM solutions now support managing Airwall Agents.

See more: [Manage Airwall Agents through an MDM \(Mobile Device Management\) solution](#) on page 70.

SD-WAN

An option was added to expose the Differentiated Services Code Point (DSCP) field of the inner IP header (plaintext) to the outer (encrypted) encapsulating header. This allows for classification of different types of network traffic for routing and prioritization purposes.

Upgrade Considerations

Consider upgrading to 2.2.8 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
Seamless bypass (split tunnel)	
Alibaba Cloud Airwall Gateways	
Set up High-availability Cloud Conductors	

New and updated Airwall help content

In addition to help for new features, here are the changes to content published since our last release:

New Topics –

- Back up Azure Airwall Gateway 300v on page 113
- Restore an Azure Cloud Airwall Gateway on page 113
- Back up your Conductor on page 112
- Restore your Conductor from a database backup on page 112

- Set the Conductor system time
- Best Practices for Conductor Configuration on page 198
- Create an Event Monitor on page 103
- See and Manage Alerts on page 102
- Set who sees Event Monitors on page 104
- Set your Email Alert Level on page 103
- The Conductor Dashboard on page 32
- Conductor Icon Reference on page 36

Updated –

- Configure Authentication Options on page 203
- Limit Device Traffic on an Airwall Gateway with Port Filtering on page 348
- How to set up Port Filtering on page 349
- What makes up an Airwall secure network? on page 119
- Deploy a Physical Conductor on page 168
- Configure a Conductor on page 198
- Create an Event Monitor on page 103
- Connect to the console port using Windows on page 251
- Set up physical Airwall Gateways on page 237
- Configure Advanced Airwall Edge Service Options on page 319
- Set up a virtual Airwall Gateway in Microsoft Hyper-V on page 261
- Allow an Airwall Agent or Server to access your Airwall secure network on page 70
- Airwall Gateway Airshell console commands – airsh on page 305

Fixes

ID	Applies to	Description
DEV-14067	Airwall GatewaysConductor	Fixed an issue on 2.2.8 Airwall Edge Services that could cause false negatives in the policy check for some overlay network configurations.
DEV-13963	Linux Airwall Server	Fixed an issue where HIP was restarting on the Linux Centos7 Airwall Server.
DEV-13754	Airwall Agent	The agent now waits for DNS to be available if the Conductor MAP address is a fully qualified domain name (FQDN).
DEV-13720	Conductor	Setting "Disable pings on active link" no longer requires a reboot.
DEV-13683	Conductor	Fixed an issue where cloud attributes smart device group rules were broken due to internal database reconfigurations. You can match devices on cloud Airwall Gateways that match certain attributes: provider, region, VPC ID, and subnet ID. For instance, you can match on "aws" to find all devices inside AWS.
DEV-13643	Airwall Gateway	Peer auto-connect setting now must be done from the Conductor. It is no longer available in Diag mode.
DEV-13627	OpenHIP	Fixed a deadlock which may occur on a busy gateway which is also acting as a relay.
DEV-13569	Airwall Gateway	Fixed excessive CPU usage when using generic Serial over IP.
DEV-13566	OSX Airwall Agent	Fixed an issue in the installer.

ID	Applies to	Description
DEV-13542	Linux Airwall Agent	The Conductor tunnel report is now working properly
DEV-13535	Conductor	Fixed an issue where Airwall agents and servers would publish transitory routing changes involving internal routing IP addresses as routing alerts in Conductor when there really was no problem. Any routing problems are still exposed via logging warnings.
DEV-13513		
DEV-13525	Airwall Gateway	Fixed an issue that caused disabling auto-repair in Linkmanager failover groups to be ignored.
DEV-13508	Conductor	Added PCI user activity entries for system level operations such as rebooting, restarting the metadata cache, and taking a database backup.
DEV-13439	Windows Airwall Agent	Fixed an issue when using Win update packages before v2.2.6 were not communicating whether they were 32- or 64-bit.
DEV-13405	Conductor	Fixed an issue where very large provisioning requests sync jobs to the licensing server were timing out.
DEV-13382	Conductor	Anonymous proxy servers are now allowed.
DEV-13353	Windows Airwall Agent	Fixed a cert error that prevented unattended installation of the Windows Airwall Agent.
DEV-13275	Airwall Gateway	Fixed an issue where a misconfigured local device can poison the ARP cache entries for peer Airwall Gateways.
DEV-13250	Airwall Gateway	You can now replace HA-paired Airwall Gateways after failure without first destroying the HA pairing.
DEV-13244	Conductor	Fixed an issue where Tag search device match rules (DMR - part of smart device groups) were not matching some matching device tags (e.g. query string of cell now matches cell1 or cellular). When adding a tag to a device that did not yet exist in the system, the DMR would miss adding the device to its group.
DEV-13217	Linux Airwall Agent	The default profile profile1 now cannot be deleted.
DEV-13213	Conductor	Fixed an issue where the Airwall Edge Service tunnel reporting data had Airwall Edge Service names truncated if they were too long. You can now see the full name by hovering over the clipped name.
DEV-13211	Windows Airwall Agent	Airwall Agent now re-enable Tempered TAP adapter on start up if it is disabled.
DEV-13209	Conductor	Ping peer Airwall Gateways now includes Airwall Gateways that are acting as both a gateway and a Relay.

ID	Applies to	Description
DEV-13207	Airwall Gateway	<p>Added the ability to specify PDP context IP type for cellular connections.</p> <p>In previous versions, the carrier-specific default was not overridden by the "ipv6" checkbox used in diag mode and airsh.</p> <p>This ipv6 checkbox has been replaced by an ip-type field, allowing customers to specify default (meaning carrier default), ipv4, ipv6, or dual-stack ipv4v6.</p>
DEV-13202	Conductor	<p>Warning log on Airwall Edge Services that monitor is unsupported when the monitor is supported have been removed.</p>
DEV-13147	OSX Airwall Agent	<p>Fixed an issue with packet captures on the OSX Airwall Agent.</p>
DEV-13134	Conductor	<p>Fixed an issue where importing an Airwall Edge Service that doesn't exist silently fails the import.</p>
DEV-13122	Android Airwall Agent	<p>Fixed an issue where failover from cellular to Wifi didn't always work without a restart.</p>
DEV-13121	Airwall Gateway	<p>Fixed an issue that caused overlay network traffic to become blocked when using the Airwall Gateway's overlay IP for serial-over-IP.</p>
DEV-13117	Conductor	<p>Now all changes to Airwall Gateway port configurations are logged in the PCI user activities log.</p>
DEV-13116	Conductor	<p>It is no longer possible to add non-local users (that is, those created in LDAP or OIDC) to a people group during creation by using Select all. You manage these people group memberships via groups in their respective systems.</p>
DEV-13107	Conductor	<p>Added PCI logging for changes to Conductor web certificate and CA chains.</p>
DEV-13101	Conductor	<p>Fixed an issue that could cause the packet capture feature in the Conductor support tab to show no capture interfaces.</p>
DEV-13100	Airwall Gateway 150	<p>Fixed an issue where upon applying certain types of port configurations, the overlay ports fail to link up until the next reboot of the airwall.</p>
DEV-13094	Airwall Gateway	<p>Fixed an issue that caused link fail-over times to be delayed by up to 30 seconds.</p>
DEV-13078	Airwall Gateway	<p>Fixed an issue that caused the reboot setting in the underlay link manager to have no effect if any underlay port groups were configured as stand-alone.</p>

ID	Applies to	Description
DEV-13077	Serial-over-IP	Fixed an issue that could cause serial-over-IP to become unresponsive after cellular outages.
DEV-13076	Conductor	Fixed a bug that could cause HIP tunnels to become stale after temporary cellular link failures.
DEV-13072	Conductor	Fixed Cellular signal strength timed out message.
DEV-13064	Conductor	Some event actions have a target box. Filtering the target box by name is now working.
DEV-13063	Conductor	Fixed a UI issue where button text wasn't visible on the HIP tunnel stats page when in Dark Mode.
DEV-13062	Conductor	Fixed a UI error when modifying the recipient list of an existing alert.
DEV-13061	Cloud	Updated paths for the 2.2.3 AW image ID in Google Cloud.
DEV-13060	Conductor	Fixed an issue where Agent hostnames were not being correctly shown for provisioning requests.
DEV-13017	Linux Airwall Agent	Fixed a non-fatal error that occurred when installing Ubuntu package on Debian.
DEV-13007	Airwall Agent	Fixed an issue where we stop sending heartbeat traffic.
DEV-13001	Android Airwall Agent	Fixed an issue where the Android Airwall Agent was sending an incorrect hostname when provisioning.
DEV-12944	Conductor	Clarified routing conflict alerts
DEV-12939	Airwall Gateway	Fixed an issue where the noUnderlayNetwork status was not set properly. This resulted in the "No underlay network" status never being displayed on LCD screens of the Airwall Gateway-400 or -500.
DEV-12932	Conductor	Fixed an issue where an Airwall Gateway generates routing alerts for east-west policy across two overlay port groups having the same subnet and overlay IP.
DEV-12906	Conductor	Fixed an issue in device activity reporting.
DEV-12892	Conductor	When there are no relay probe diagnostic results, a message now indicates that it is because the Airwall Gateway is not a member of any relay rules. Furthermore, fixed an issue where a value in the diagnostic data was misidentified as latency. In reality, this value is a score used to determine which relay to use. A lower score is better.
DEV-12882	Conductor	Airwall Gateways that use stand-alone underlay port group configurations now reboot on link failure if the reboot feature is enabled.
DEV-12859	Airwall Gateway	Removed extra repeated log messages that occurred when Airwall Gateway-300v did not have a virtual serial port attached.

ID	Applies to	Description
DEV-12858	Conductor	Fixed an issue where duplicate results in relay probe diagnostic data result from multiple interfaces attempting to connect to the relay. The Conductor now only shows the best results.
DEV-12855	Airwall Gateway	Fixed an issue where when reconfiguring overlay port groups the DHCP server / relay was not restarted.
DEV-12828	Windows Airwall Agent	Fixed an install issue with Windows 32-bit Airwall Agent.
DEV-12778	Windows Airwall Agent	Installation timestamp now fixed in Conductor.
DEV-12755	Conductor	Fixed an issue where User auth overlay membership was not correctly published in all cases when people were added and removed from people groups.
DEV-12731	Conductor	HA-paired relays are now correctly named in the relay probe diagnostic tool.
DEV-12727	Airwall Gateway	Fixed an issue where a relay was giving a "Relay could not find an IPv4 source address" error.
DEV-12710	Airshell	Fixed an issue in Airshell where multiple cellular parameters could not be configured in one command.
DEV-12701	Airshell	When using Airshell, if the Airwall Gateway is in Diagnostic Mode, networking is not automatically restarted when configuring underlay address ('conf network') or modem settings ('conf cell').
DEV-12697	Airshell	Fixed an issue where the Airshell log command does not display the log file on virtual Airwall Gateways.
DEV-12684	Conductor	When looking at voucher details, license model names are now in the same format as those on the licensing page.
DEV-12662	Airwall Gateway	Fixed an issue where Airwall Gateways equipped with Quectel cellular modems did not properly report signal strength on the front-panel LEDs.
DEV-12648	Airwall Gateway	Fixed an issue where the Airwall Gateway-150 USB console port USB descriptor reported that the port is AT command capable, causing ModemManager on Debian to probe the port as if it were a modem.
DEV-12608	Airwall Gateway	Fixed an issue in firmware 2.2.3 and 2.2.5 where the SFP LEDs on the Airwall Gateway 150 remain on when the SFP port is not in use in some configurations.
DEV-12566	Conductor	People groups created as a result of logging in via an authentication provider are now part of the PCI log.
DEV-12559	Conductor	In the smart device group dialog, when "Ignore auto-discovered devices until accepted" is turned off, the group now picks up any existing discovered devices that match its rules.
DEV-12505	Conductor	New PCI logs for Airwall Edge Services reconnect support function, starting a PCAP, stopping a PCAP, requesting a support bundle, and requesting a diagnostic report.

ID	Applies to	Description
DEV-12496	Conductor	Fixed an issue where event actions could have a text display error if you edit one action while editing another.
DEV-12434	Conductor, Airwall Gateway	Now have support for NATing subnet broadcasts on the device network.
DEV-12232	Airshell	The two logins available on both Airwall Gateways and Conductor are "airsh" and "diag". All previous logins have been removed.
DEV-11810	Conductor	The Conductor now displays a more helpful error page for Conductor session timeout.
DEV-11806	Cloud	Cloud Diagnostics page Refresh button now refreshes the Protected Route table.
DEV-11795	Linux Airwall Agent	Fixed an issue where the current profile is not changed as a result of an update.
DEV-11679	Airwall Gateway	Fixed an issue where HA configured Airwall Gateways did not support the overlay DHCP feature after a fail-over.
DEV-11408	Android Airwall Agent	Fixed an issue where an Android Airwall Agent failed to connect with peers if it had policy to network objects.
DEV-10081	Conductor	Fixed an issue in the Create Conductor certificate dialog where hitting Enter didn't save the certificate.
DEV-8347	Windows Airwall Agent	Windows Support Bundles are now encrypted.

Known Issues

ID	Applies to	Description
DEV-14197	MacOS Airwall Agent	When you update the macOS Airwall Agent, you may be required to restart. If you don't see the tray icon after the update finishes, restart your Mac to restore operation of the Airwall Agent.
DEV-13944	Airwall Gateway	When a device is disabled it will only stop traffic to other devices on remote Airwall Gateway's. Traffic to bypass destinations will continue. Traffic to other devices on the same Airwall Gateway will not be stopped in some situations.

ID	Applies to	Description
DEV-13930	Alibaba Cloud Airwall Gateway, Conductor	<p>If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet.</p> <p>Workaround: You can avoid this issue by waiting to install the upcoming 2.2.8 hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways.</p> <p>Workaround if you have already created an Alibaba Cloud Airwall Gateway:</p> <ol style="list-style-type: none">1. Apply this hotfix to your Conductor.2. If you are not using an NTP for system time, on the Settings page, General setting tab, under System time, select Edit Settings, and then Under Update date and time, select Set browser time and then select Update.3. For any cloud Alibaba Airwall Gateways, on the Cloud tab, Diagnostic subtab, click Refresh.

ID	Applies to	Description
DEV-13916	Airwall Gateway	<p>Airwall Gateways running firmware version 2.2.8 will not use a Conductor URI that was previously learned from a DNS SRV record in v2.2.8 or a previous firmware revision.</p> <p>This leaves the Airwall Gateways unable to connect to the Conductor if the Airwall Gateway previously used a DNS SRV record for configuration and is later moved to a network without a Tempered DNS SRV record.</p> <p>Additionally, the Conductor setting that allows you to set the Conductor URI on all managed Airwall Gateways in Advanced Settings is not functional when used with DNS SRV record bootstrapping in firmware v2.2.8.</p> <p>Workaround: Prior to installing 2.2.8 on Airwall Gateways, install Hotfix-13955. You can then install 2.2.8 on the Airwall Gateways.</p> <p>If you have already installed 2.2.8 on Airwall Gateways and are experiencing this issue, please contact support@tempered.io for assistance, or you can manually configure the Conductor address in each Airwall Gateway using <code>airsh</code> or Diagnostic mode.</p>
DEV-13913	Alibaba Cloud	<p>The 2.2.5 Airwall Gateway image in Alibaba Cloud deploys a 2.2.3 image instead.</p> <p>Workaround: After you finish deploying, upgrade the Airwall Gateway to the version you want.</p>
DEV-13887	Windows Airwall Agent or Server	<p>There is an issue on some Windows machines where the Windows Airwall Agent or Server can't connect, even though ipconfig shows an auto-configured IP address for the Tempered TAP adapter (169.254.*.*), and the Conductor shows the device as online but with no IP address.</p> <p>Workaround:</p> <p>Restart the service, or check your Airwall Agent or Server configuration in the Conductor.</p>
DEV-13872	Conductor	<p>When running Ping all devices on the Support tab for a HA standby Airwall Gateway, no results are being displayed and the busy status indicator never times out.</p>

ID	Applies to	Description
DEV-13860	Conductor	If you add a device when multiple port groups are already configured, the Port affinity list defaults to the first overlay port group, but the value set is "Detect automatically." Workaround: Edit the device again and change it to set port affinity.
DEV-13846	Conductor	Network admins cannot get the list of CAs and cannot add customer certificates to Airwalls through the UI, because the PKI button is not shown.
DEV-13813	Airwall Gateway 110g	RS-422 / RS-485 functionality is not guaranteed on the Airwall 110 for the 2.2.8 release.
DEV-13811	Airwall Gateway	When using an Airwall Gateway to provide high availability across multiple underlay links, do not place multiple interfaces in the underlay port groups or use bypass with routed-only mode disabled.
DEV-13775	Cloud	The Conductor rarely gives a "Net::ReadTimeout" error when you try to deploy an Azure Airwall Gateway 300v or server. This error doesn't indicate that the deployment has failed – go to the Azure portal and check the actual deployment result.
DEV-13760	Conductor	Device page export/import does not export or import Bypass Devices in this release.
DEV-13759	Airwall Gateway	Detect Devices button may incorrectly report devices on attached to other port groups or peer Airwalls if policy permits traffic from an Overlay IP to those destinations.
DEV-13607	Conductor	Creating a link failover group (Airwalls -> Ports -> Failover settings) does not apply the settings to any port groups. This is easy to miss since you have to set the failover group on the ports page.
DEV-13297	Airwall Gateway	When deploying seamless bypass in a layer 2 "bump in the wire" configuration, traffic from the protected device to non-bypass destinations outside of the local subnet does not work as expected. The traffic egresses the remote Airwall Gateway or other port group with the destination MAC address of the local default gateway. Using seamless bypass in layer 2 "bump in the wire" mode to provide remote access to the protected device with and overlay IP and SNAT enabled works as expected.
DEV-13194	Conductor	An Airwall Edge Service's Check Connectivity / Ping Local Devices functionality can fail in Internet Explorer 11 if one of the devices is defined as a CIDR. To fix this, use one of the latest versions of Chrome, Firefox, Safari or Edge.

ID	Applies to	Description
DEV-12852	Windows Airwall Agent	<p>The Windows Airwall Agent may not connect when multiple interfaces are active.</p> <p>This issue can be caused by a Windows default that doesn't allow multiple simultaneous active network interfaces, and prefers ethernet over cellular or WiFi. It can be bypassed by editing a registry value. See the troubleshooting steps in I'm having trouble connecting on page 31.</p>
DEV-12744	Airwall Gateway	<p>Customers with Airwall Agents version 2.2.1 or earlier connecting to HA-paired Conductors might not be able to authenticate a user auth session.</p> <p>Recommendation: Upgrade Conductors and Airwall Agents to version 2.2.3 or above.</p> <p>Workaround: After upgrades, if you still see connectivity issues, restart the Airwall Agent.</p>
DEV-12692	API Documentation	<p>The API docs navigation section does not work in chrome 80 though it worked on previous versions of chrome. It is still working in Firefox and Safari, so customers should use one of these browsers to view the docs.</p>
DEV-12544	Conductor	<p>If you restore a Conductor using a VM snapshot, and it is part of an HA pair, the Standby must be rebased as the standby. To do this, set the Standby Conductor to Active, and then back to Standby. This generates a new Standby Database.</p>
DEV-12513	Cloud-Azure	<p>Conductor rarely gives a "Net::ReadTimeout" error when user tries to deploy an Azure Airwall Gateway 300v or server. This doesn't indicate that the deployment has failed. If you get this error message, go to the Azure portal and check the actual deployment result.</p>
DEV-12275	OSX Airwall Agent	<p>DNS settings are seen and acted upon, but don't show up in resolver list.</p>
DEV-12264	Airwall Agent	<p>Revoking and then re-activating an Agent on a Conductor before v2.2.8 results in the Agent being unable to reconnect.</p> <p>Restarting the metadata cache on the Conductor resolves this issue.</p>
DEV-11840	Conductor	<p>Attempting to log into a Standby Conductor with an expired password cycles into a recycling change password prompt. If this occurs, log into the Active Conductor to change the password.</p>
DEV-11523	Conductor	<p>In rare cases, the Airwall Edge Services online/offline status graph on the Dashboard might be blank.</p>

ID	Applies to	Description
DEV-10977	Cloud	If one of the cloud attributes is missing, please reboot the Airwall Gateway by clicking the Airwall Gateway -> Actions -> Reboot.
DEV-10846	OSX Airwall Agent	On OSX Airwall Agents, it may not be possible to stop an ongoing packet capture. Workaround: Wait for the capture duration to expire.
DEV-10710	Conductor	Supported platforms for Upgrade are not listed in order in Conductor
DEV-10276	Windows Airwall Agent	Tray Application doesn't start on Server 2008 because .NET fails to install silently.
DEV-8486	Conductor	Clicking the Restart IF-MAP button will log the current user out.
DEV-8120	Conductor	Infrequently, an Azure Airwall Gateway may fail to reconnect to Conductor after firmware upgrade. This can be fixed by going to the Azure portal and restarting the VM the Airwall Gateway resides on. It can take up to 10 or 15 mins to come back online.

Release Notes 2.2.5

Release Date: Apr 17, 2020

What's New

Support for NAT Subnet Broadcasts

The Airwall Solution now supports NATing subnet broadcasts on the device network.

New Airwall help content

- [Airwall Invitations](#)
- [Renew Expired Licenses](#)
- [Integrate Third-party Authentication with OpenID Connect](#)
- [Set up an Airwall Gateway in Microsoft Azure](#)

Updated Airwall help content

- [Configure a DHCP relay on an Airwall Gateway](#)
- [Configure protected devices with DHCP](#)
- [Route encrypted connections with Airwall Relay](#)
- [Configure Airwall Relay rules](#)
- [Install Airwall Server on Linux](#)

Upgrade Considerations

Consider upgrading to 2.2.5 if:

You were impacted by any issues discovered in prior releases, especially if you have any of the following:

Heavy use of broadcast/multicast traffic.
Applying a new ports configuration resulted in overlay ports staying down until next reboot.
Tunnel failures after cellular outages.

Fixes

ID	Applies to	Description
DEV-13132	Conductor	Improved validation of Conductor device imports.
DEV-13087	Android Airwall Agent	Fixed an issue where user was unable to log in with user auth on Android.
DEV-13086	Conductor	Airwall port configuration changes made from the Conductor are now noted in the PCI user activities log
DEV-13067	Android Airwall Agent	Fixed Push-to-Talk not working on Android over Cellular.
DEV-13065	Android Airwall Agent	Fixed Android issue with sending User Auth credentials causing crashes.
DEV-13031	Conductor	Agent hostnames are now being shown correctly for provisioning requests.
DEV-12954		
DEV-13027	Conductor	Added new PCI logs for Airwall reconnect support function: Starting a PCAP, stopping a PCAP, requesting a support bundle, and requesting a diagnostic report.
DEV-13002	Airwall Gateway	Fixed an issue that caused the reboot setting in the underlay Failover Settings tab to have no effect if any underlay port groups were configured as standalone.
DEV-12938		
DEV-12998	Conductor	Fixed an issue that could cause the packet capture feature in the old Conductor support tab to show no capture interfaces.
DEV-12930		
DEV-12997	Conductor	Fixed an issue that could cause serial-over-IP to become unresponsive after cellular outages.
DEV-12996	Conductor	Fixed an issue to allow users to request multiple support bundles at the same time.
DEV-12995	Conductor	Fixed a bug that could cause HIP tunnels to become stale after temporary cellular outages.
DEV-12871		
DEV-12994	Conductor	Some event actions have a target box. Filtering the target box by name is now working. Additionally you can select "+ more" to see more entries at the same time.
DEV-12866		

ID	Applies to	Description
DEV-12992	Conductor	Fixed a UI error when modifying the recipient list of an existing alert.
DEV-12083		
DEV-12991	Android Airwall Agent	Fixed Android Airwall Agent sending localhost as the hostname in its provisioning request.
DEV-12984	Airwall-75 Airwall-150 Airwall-250	Fixed an issue where applying certain types of port configurations caused the overlay ports fail to link up until the next reboot of the Airwall. Note: This issue may still occur in a configuration where only VLAN-tagged ports are assigned to overlay port groups. To work around this, ensure that at least one untagged port is assigned to an overlay port group.
DEV-12964	Airwall Gateway	Fixed a bug that caused the reporting interval settings to have no effect on device activity reporting.
DEV-12903	Conductor	Fixed an issue where syslog didn't configure the first time on a new Conductor.
DEV-12748	Conductor	Fixed an issue where an Airwall may crash when processing a large amount of broadcast traffic with many tunnels.

Known Issues

ID	Applies to	Description
DEV-13028	Airwall Gateway	Airwall Gateway 150 has "could not detect attached switch" error. Workaround: Do a hard reboot.

Release Notes 2.2.3 Hotfix

Release Date: Mar 27, 2020

What's New

2.2.3 Hotfix

This is a hotfix to release v2.2.3. See the [Release Notes 2.2.3](#) for more additions in version 2.2.3.

Upgrade Considerations

We recommend that you upgrade to this 2.2.3 hotfix if you were impacted by issues with the Windows or macOS Airwall Agents.



Note: If you're looking for the previous Tempered Networks Technical Documentation, most is included in the new Airwall Help. You can also click the link on the [Airwall Help](#) home page to get to the pre-2.2.3 Help.

Fixes

ID	Applies to	Formerly Known As	Description
DEV-12954	Conductor		Agent hostnames were not being correctly shown for provisioning requests.

ID	Applies to	Formerly Known As	Description
DEV-12938	Airwall Gateway	HIPswitch	We fixed an issue that caused the reboot setting in the underlay link manager to have no effect if any underlay port groups were configured as stand-alone.
DEV-12930	Conductor		We fixed an issue that could cause the packet capture feature in the Conductor support tab to show no capture interfaces.
DEV-12871	Conductor		We fixed a bug that could cause HIP tunnels to become stale after temporary cellular link failures.
DEV-12866	Conductor		Some event actions have a target box. Filtering the target box by name is now working. Additionally you can select "+ more" to see more entries at the same time.
DEV-12852	Windows Airwall Agent	HIPclient-Windows	Windows Airwall Agent wasn't handling re-address during interface (for example, cell to wifi) changes
DEV-12803	Conductor		UI error when modifying the recipient list of an existing alert.
DEV-12755	Conductor		User auth overlay membership was not correctly published in all cases when people were added and removed from people groups.

Known Issues

See [Release Notes 2.2.3](#) on page 554 for known issues.

Release Notes 2.2.3

Release Date: Feb 6, 2020

Introducing Tempered Airwall

Tempered's fully encrypted, virtual air-gap network security solution is now called Airwall. Our product offerings are also changing to match our brand and make their functions clearer.

What's New

New Airwall help

If you're looking for the previous Tempered Networks Technical Documentation, most is included in the new Airwall Help. You can also click the link on the home page to get to the pre-Airwall Help.

OpenID Connect support for Airwall Agents

We have added OpenID Connect support for authenticating remote sessions on Android, iOS and macOS Airwall Agents (formerly Android, iOS, and OSx HIPclients). There is also now a global option to lock out clients that do not support user auth.

People groups as Overlay members/managers

People Groups are now able to be members of Overlay Networks as well as Managers of Overlay Networks. Now user permissions can be configured entirely in an authentication provider such as LDAP or OpenID Connect via people group membership.

Lockdown Mode

Lockdown Mode is now configurable from the Airwall Conductor for Airwall Agents (formerly HIPclients) that support this feature (currently supported by the Windows Airwall Agent).

Cloud Linux Airwall Servers

The Airwall Conductor can create and deploy Linux Airwall Servers directly in any cloud provider, such as Azure, AWS, or Google.

Upgrade Considerations

We recommend that you upgrade to 2.2.3 if:

You want to use any of the following features: Multifactor Authentication	You were impacted by any issues discovered in prior releases, especially if you have any of the following: <ul style="list-style-type: none"> • A large number of spokes causes network issues • Issues with NTPD (Network Time Protocol daemon) not running on Conductor • Broadcast traffic not forwarded across Overlay network
--	--



Important: If you are using SHA-1 for the ESP transform, you should convert to SHA-256 before upgrading to 2.2.x.

IMPORTANT: Migrating existing Deployments to 2.2.x

The 2.2.2 release brought a significant change to the base platform configuration and capabilities of an Airwall Gateway/HIPswitch. Conductors after 2.2.2 will not be able to manage Airwall Edge Services prior to version 2.0. See the note in the [Release Notes 2.2.2](#) on page 563 for information on upgrading Airwall Edge Services prior to version 2.0.

Fixes

ID	Applies to	Formerly Known As	Description
DEV-12852	Windows Airwall Agent	HIPclient-Windows	Windows Airwall Agent wasn't handling re-address during interface (for example, cell to wi-fi) changes
DEV-12683	Airwall Gateway	HIPswitch	Fixed an issue where large firmware update packages would sometimes fail to be installed via Conductor, Diagnostic mode, and airsh (hipsh).
DEV-12613	Airwall Gateway-250	HIPswitch-250	Fixed an issue where port 8 (SFP portion) of the Airwall Gateway-250 does not get re-enabled after reconfiguring network interfaces. This issue affects firmware versions 2.2.0, 2.2.1, and 2.2.2.

ID	Applies to	Formerly Known As	Description
DEV-12582	iOS Airwall Agent	HIPapp-iOS	iOS Airwall Agent - 2x 'Sign-in Failed' pop up for invalid username & password
DEV-12579	iOS Airwall Agent	HIPclient-iOS	iOS Airwall Agent not using 'DNS domain' from Conductor
DEV-12528	Android and iOS Airwall Agents	HIPclient-Android HIPclient-iOS	Android and iOS Airwall Agents user auth status pages are not getting updated on toggling policies
DEV-12510	Android Airwall Agent	HIPclient-Android	Android and iOS Airwall Agents user auth status pages are changing session expire time according to the current time of the phone.
DEV-12487	Android Airwall Agent	HIPclient-Android	Android Airwall Agent user auth Notification showing symbols instead of profile name
DEV-12468	Android Airwall Agent	HIPclient-Android	Android Airwall Agent crash on overlay networks page when you click refresh with no peers
DEV-12463	Conductor		Syslog setting appears disabled after upgrade while it is still enabled
DEV-12441	Linux, macOS, and Windows Airwall Agents OpenHIP	HIPclient-Linux, HIPclient-OSX HIPclient-Win	Mac, Linux and Windows Airwall Agents now use and select an optimal relay when the underlay interface is set to 'auto'.
DEV-12404	Airwall Gateway-150	HIPswitch-150	A new cellular modem firmware (version 02.33.03.00) is available for Airwall Gateway-150 with the SFF-MOD-MC7430 modem. Please see the downloads page .
DEV-12399	OpenHIP		Reject ARP responses for loopback, multicast, broadcast and 0.0.0.0
DEV-12382	Conductor		Airwall Edge Services online bar graph displays, then goes blank.
DEV-12376	Conductor		HTTP 422 error for some accounts after 2.2.1 > 2.2.2 Conductor upgrade.
DEV-12373	iOS Airwall Agent	HIPclient-iOS	iOS status page seems to not be updating
DEV-12355	OpenHIP		Broadcast IP packets not traversing tunnel properly
DEV-12353	Airwall Gateway-150	HIPswitch-150	Some Airwall Gateway-150s with part numbers (PLF-) ending in -02 and -03 were shipped with non-functional SFP ports due to a firmware bug. This is fixed in firmware version 2.2.3. Additionally, a hotfix is available to address this issue in firmware versions 2.1.6, 2.1.7, 2.2.0, 2.2.1, and 2.2.2.

ID	Applies to	Formerly Known As	Description
DEV-12339	Airwall Gateway-150	HIPswitch-150	A regression in firmware versions 2.2.0, 2.2.1, and 2.2.2 caused Airwall Gateway-150s to be unable to link with dual-speed or BiDi SFP/SFP + modules. Support for these SFPs is fixed in firmware 2.2.3.
DEV-12326	Conductor		Airwall Edge Services fail to reconnect to Conductor after re-provisioning
DEV-12318	Android Airwall Agent	HIPclient-Android	Android not using 'DNS domain' from Conductor
DEV-12311	Airwall Gateway	HIPswitch	Fixed an issue that was causing serial or modbus configured overlay ports to stop working after performing a reconnect.
DEV-12301	Airwall Gateway	HIPswitch	Fixed a bug that caused Airwall Gateways to lose their Conductor connection after installing a customer certificate requiring a reboot.
DEV-12293	Airwall Gateway	HIPswitch	Modbus-RTU times out when multiple sessions are connected from one host.
DEV-12287	Airwall Gateway-500	HIPswitch-500	Fixed a bug that caused some IP broadcasts on the overlay network to cross into different subnets.
DEV-12285	macOS Airwall Agent	HIPclient-OSX	Mac unable to log in via username and password after switching to a different profile
DEV-12276	Conductor		Do not allow a non-editor to be the rule editor of a Smart Device Group.
DEV-12241	iOS Airwall Agent	HIPclient-iOS	iOS needs to initiate pings for other side to reach it
DEV-12230	Airwall Gateway	HIPswitch	Do not remove port group configs during port detection
DEV-12219	OpenHIP		When processing concurrent traffic to or from multiple peers an Airwall Gateway may drop traffic for some tunnels.
DEV-12217	Airwall Invitations	HIPinvite	Poor messaging of license sync errors during invite activation
DEV-12214	Conductor		Monitor alert (flapping) settings do not result in an indication of frequent alerts
DEV-12205	Conductor		Not able to remove NTP on the Standby
DEV-12187	Conductor		Airwall Edge Services uptime graph units scale incorrectly
DEV-12179	Conductor		Deleting SoIP/Modbus settings when a description is edited
DEV-12167	Conductor		Remove tags and end remote session on revoke
DEV-12159	Conductor		Doesn't log device traffic reported by High-Availability standby

ID	Applies to	Formerly Known As	Description
DEV-12146	Windows Airwall Agent	HIPclient-Win	Windows Airwall Agent takes a very long time to appear in Conductor dashboard after license is granted
DEV-12127	OpenHIP		Detect unidirection traffic through tunnels which may indicate an extremely rare issue that causes tunneled traffic to be lost and attempt to recovery tunnel by initiating a rekey
DEV-12104	Conductor		Change license pop up blocking functionality to a temporarily dismissible banner
DEV-12096	Airwall Gateway	HIPswitch	Address Marvell WiFi "mwifiex" driver CVEs: CVE-2019-3846, CVE-2019-14814, CVE-2019-14815, CVE-2019-14816, and CVE-2019-14895
DEV-12093	Android Airwall Agent	HIPclient-Android	Add DNS setting back to Android and iOS Airwall Agents
DEV-12092	Airwall Gateway-150	HIPswitch-150	Airwall Gateway-150 not maintaining HIP tunnels when configured with more than 10 peers
DEV-12090	OpenHIP		In previous versions, HIP would buffer packets during the base exchange. This has been removed to mitigate a potential DoS from a local protected device, almost all protocols will re-transmit making the buffering unnecessary. If you encounter issues with esoteric protocols, please turn on auto-connect so the tunnels are brought up automatically.
DEV-12077	Airwall Gateway	HIPswitch	If fail-safe reboot is enabled in the Failover settings, the Airwall Gateway reboots whenever the initial reboot timeout is expired (assuming all links failing) ignoring the timeout for recurring reboot.
DEV-12076	Conductor		Invalid license vouchers shouldn't prevent customers from loading new valid vouchers
DEV-12075	Licensing		Customer cannot remove invalid licenses due to license deficit
DEV-12024	Airwall Gateway-150	HIPswitch-150	Fixed a bug that was causing validation errors in the port configuration UI after factory-resetting and re-connecting an Airwall Gateway to the same Conductor.
DEV-12005	Conductor		Device Match Rules rule "include Any Object without certain tag" does not include untagged devices
DEV-12004	Conductor		Device Match Rules "negative filter MAC_prefix" filters out devices without MAC address
DEV-12000	Conductor		Offline Airwall Agents are named incorrectly in Add Device to Network popup

ID	Applies to	Formerly Known As	Description
DEV-11994	Conductor		Replacing Airwall Agent in Conductor doesn't update its capabilities
DEV-11992	Conductor	Conductor	Conductor breaks when upgrading to from 2.2.1 to 2.2.2 in a factory reset state.
DEV-11991	Airwall Gateway	HIPswitch	Fixed an issue that causes dropped packets when traffic from the same MAC address is received on multiple ports of the same Airwall Gateway (regardless of the port group membership of those ports).
DEV-11982	Conductor		The auto-generated Lockdown Mode Device Group doesn't appear to match new Airwall Gateways coming online.
DEV-11969	Conductor		NTPD terminates and won't come back.
DEV-11968	Cloud		Delay and fetch userdata causes slow Conductor refresh
DEV-11951	Conductor		Notifications Controller Validation failed: MTU must be greater than or equal to 100 when no MTU provided by 2.2.2 HIPapp
DEV-11900	Airwall Gateway	HIPswitch	Modbus-RTU does not work correctly when Overlay NAT is enabled.
DEV-11898	Android and iOS Airwall Agents	HIPclient-Android, HIPclient-iOS	Unable to establish any Overlay connections with Android and iOS Airwall Agent
DEV-11893	Android Airwall Agent	HIPclient-Android	Scale views on Overlay and Services page in Airwall Agent
DEV-11887	Android Airwall Agent	HIPclient-Android	In Add Profile, error remains after you correct the field
DEV-11881	Conductor		Keep user auth timeout within the range of 1 hour to 1 year
DEV-11867	Airwall Gateway	HIPswitch	Ruggedcom: Cannot enter diagnostic mode from hipsh (now airsh)
DEV-11864	Airwall Gateway-150	HIPswitch-150	Fixed an Airwall Gateway-150 issue where the cellular LED indicators did not function properly following the first reboot after inserting the AW-150 cellular module.
DEV-11858	Conductor		End Remote Session button activity is missing from PCI user activities
DEV-11844	Conductor		Blank Provider name for OpenID connect leads to blank dropdown list item
DEV-11830	Conductor		Able to authenticate user auth using expired password
DEV-11829	Conductor		Unable to log in legacy users without email

ID	Applies to	Formerly Known As	Description
DEV-11824	Conductor		Deleting the people group doesn't remove the tag from the Airwall Edge Services
DEV-11823	Android and iOS Airwall Agents	HIPclient-Android, HIPclient-iOS	Prevent users from clicking multiple times on Login and Sign in
DEV-11819	macOS Airwall Agent	HIPclient-OSX	Doing anything in the macOS Airwall Agent closes your user auth session
DEV-11815	Conductor		Add notice or block transparent mode when multiple overlay port groups are configured.
DEV-11807	Airwall Gateway	HIPswitch	Ping all devices on High-Availability Standby in failover mode
DEV-11804	Cloud		Route injection was not performed on Conductor reboot or upgrade
DEV-11794	Linux Airwall Agent	HIPclient-Linux	WiFi scanning is now available on the Linux Airwall Agent
DEV-11785	Conductor		Conductor should remove remote session button on disabling global user auth
DEV-11778	Airwall Gateway	HIPswitch	HTTP GET overlay monitor confused when multiple port groups
DEV-11772	iOS Airwall Agent	HIPclient-iOS	iOS Airwall Agent user auth alert icon on Dashboard doesn't work on click
DEV-11769	iOS Airwall Agent	HIPclient-iOS	iOS Airwall Agent not getting overlay device IP updates
DEV-11733	Conductor		Airwall Gateway High-Availability, you get incorrect status after failover: primary Airwall Gateway status reports OK (tunneling)
DEV-11732	Airwall Gateway-150	HIPswitch-150	Fixed an issue where Quectel cellular expansion modules would sometimes fail to connect to AT&T's LTE network and instead fall back to 3g / UMTS.
DEV-11727	Licensing		Denied license request not cleared after import of synced encrypted package
DEV-11698	Airwall Gateway-300v HA	HIPswitch-300v	Airwall Gateway-300v High-Availability member went offline after removing High Availability settings
DEV-11684	Conductor		Starting concurrent packet captures on the same Airwall Gateway appears to work, then fails with "An error occurred communicating with the server"
DEV-11680	Android Airwall Agent	HIPapp-Android	Airwall Agent Invitations Decline and Conductor hidden in landscape view
DEV-11677	Conductor		Conductor ports config permits network address as overlay IP

ID	Applies to	Formerly Known As	Description
DEV-11656	Airwall Gateway-150	HIPswitch-150	In firmware versions 2.2.0, 2.2.1, and 2.2.2, a regression caused the link LEDs for Airwall Gateway-150 port 5 (SFP) to not operate when port 5 is assigned to an Overlay port group. This is fixed in firmware version 2.2.3. Note: The SFP port LEDs turn on and stay solid when the Airwall Gateway has not been managed in a Conductor. This issue will be addressed in a future release.
DEV-11651	Conductor		Airwall Gateway Ports page doesn't display IP or MAC address after configuring
DEV-11645	Conductor		OpenID user auth login requires re-authentication
DEV-11516	Conductor		Device import allows device with arbitrary name/description length
DEV-11499	iOS Airwall Agent	HIPclient-iOS	iOS Airwall Agent shows LSI for NAT'd devices on overlay networks page
DEV-11470	Airwall Agents Airwall Servers	HIPclients HIPservers	Changing overlay IP conf. back to NAT requires Airwall Agent restart
DEV-11459	Conductor		iOS Airwall Agent doesn't show up on Conductor
DEV-11343	Airwall Gateway	HIPswitch	The port detection part of hardware detection was made more reliable, for upgrades and during each boot on certain platforms.
DEV-11103	Conductor		A device's port group can now be seen and edited from the Airwall Gateway's "local devices" tab.
DEV-11013	macOS Airwall Agent	HIPclient-OSX	Switching profile doesn't forget about user auth sign-in
DEV-10960	macOS Airwall Agent	HIPclient-OSX	If you add wrong credentials for user auth on macOS, it won't ask you to enter again
DEV-10887	Linux Airwall Server	HIPserver-Linux	Linux Airwall Server DNS server settings don't seem to have any effect
DEV-10665	macOS Airwall Agent	HIPclient-OSX	macOS 10.15 requires app notarization by default
DEV-10592	Cloud-Azure		Don't require reboot to get the route table ID
DEV-10555	Cloud-AWS		Better user error for auth failure due to time difference
DEV-9927	Linux, macOS, and Windows Airwall Agents Airwall Gateways	HIPclient-Linux HIPclient-OSX HIPclient-Win HIPswitch	Mac Airwall Agent receives routes for disabled overlays
DEV-9857	iOS Airwall Agent	HIPclient-iOS	Don't allow access to private key when phone is locked

ID	Applies to	Formerly Known As	Description
DEV-9253	Conductor		Smart Device Groups will not add Airwall Agents and Airwall Servers using tag matches.
DEV-9204	Conductor		Airwall Gateway Underlay IP NAT field shouldn't accept CIDRs
DEV-9122	macOS Airwall Agent	HIPclient-OSX	macOS Airwall Agent publishes IP of random interface as an Underlay IP
DEV-8929	Windows Airwall Agent	HIPclient-Win	Tray app doesn't start after unattended install
DEV-8742	Conductor		Add better error messaging for the initial Conductor voucher failures

Known Issues

ID	Applies to	Formerly Known As	Description
DEV-12744	Airwall Gateways	HIPswitches	Customers with Conductor HA and Airwall Gateways version 2.2.1 or earlier might see connectivity issues when using User Authentication. Recommendation: Upgrade Conductors and Airwall Gateways to version 2.2.3 Workaround: After upgrades, if you still see connectivity issues, restart the primary Conductor.
DEV-12710	airsh	hipsh	Customers need to update each cell value individually when using airsh to configure the cell modems
DEV-12697	airsh	hipsh	The console command "airsh log" does not display the log file on a virtual Airwall Gateway. The 300v log file is now located at /etc/asguard/system/messages.
DEV-12692	API		The API docs navigation section does not work properly in Chrome v80. Use Firefox or Safari to view the API docs.
DEV-12645	Android Airwall Agent	HIPClient-Android	When creating a new profile and starting the app for the first time there is a chance the "Upgrade Needed" page will be displayed. This is an error and the user should simply click cancel and start the app again. This may only happen the first time you create the profile.
DEV-12521	Airwall Gateway	HIPswitch	TPM usage is disabled by default for all Airwall Gateways due to the amount of time it takes to complete an RSA signature and frequency of RSA signatures when connected via a relay. This will be addressed in a future version.

ID	Applies to	Formerly Known As	Description
DEV-12513	Cloud Azure		Conductor occasionally gives "Net::ReadTimeout" error when user tries to deploy an Azure Airwall Gateway 300v or server. This doesn't indicate that the deployment has failed. Go to the Azure portal and check the actual deployment result.
DEV-12303	macOS Airwall Agent	HIPclient-OSX	Upgrading macOS Airwall Agent from 2.2.1 to 2.2.3 requires uninstalling the 2.2.1 Airwall Agent, installing the 2.2.3 Airwall Agent, and replacing the old profile with new profile on Conductor.
DEV-12290	macOS Airwall Agent	HIPclient-OSX	User approval needed to complete macOS Airwall Agent installation. From macOS High Sierra onwards, you need to allow the system extension com.tempered.tuntaposx.tap, or simply tap.kext, required by the Airwall Agent. In the System Preferences, on the Security and Privacy page, open the General tab. Where it says system software was blocked from loading, click Allow . macOS only shows this allow message for a limited time (30mins). The installer will wait for you to allow the extension.
DEV-12268	Conductor		Firmware version on Conductor is not getting updated until macOS Airwall Agent is restarted
DEV-11578	Android Airwall Agent	HIPclient-Android	Do not change the LSI prefix to match a peer address.
DEV-9542	iOS Airwall Agent	HIPclient-iOS	Cannot generate a Support Bundle from the Conductor for an iOS Airwall Agent when the Conductor is in High Availability mode. You can instead generate a Support Bundle from the iOS Airwall Agent

Older Release Notes

Release Notes for versions 2.1.2 through 2.2.2.



Note: For v2.0.3 and earlier, see [pre-2.2.3 Tempered Webhelp](#) for release notes for earlier versions.

Release Notes 2.2.2

Release Date: October 18 , 2019

IMPORTANT: Customers using LDAP on Conductor 2.2.1

If you are using LDAP and running Conductor version 2.2.1, you must upgrade your Conductor to 2.2.2, to resolve an issue that could prevent you from logging in to the Conductor.

IMPORTANT: Migrating existing Deployments to 2.2.2

The 2.2.2 release brings a significant change to the base platform configuration and capabilities of a HIPswitch. HIPswitch versatility is dramatically increased. To achieve this, we had to give up some functional interoperability between version 2.2.2 and prior versions of HIPservices and Conductor. Also, Conductor 2.2.2 will no longer be able

to manage HIPservices prior to version 2.0. While most things still work across versions 2.1.x and 2.2.2 during your upgrade, we recommend that 2.2.x deployments migrate completely as soon as possible using the following order:

1. If your Conductor is running a version earlier than 2.1.6, upgrade it to 2.1.6 or 2.1.7
2. If any HIP Services are running a version earlier than 2.1.6, upgrade them to 2.1.6 or 2.1.7
3. Verify that your Conductor and all HIP Services you updated in steps 1 and 2 are running 2.1.6 or later
4. Upgrade your Conductor to 2.2.2
5. Upgrade your HIP Services to 2.2.2

For more information on upgrading your Conductor to 2.1.6 from prior versions, log in to your account and select the **Documentation Center** link at the top-right of the page. You should review both the **Release Notes 2.1.6** and **Conductor and HIP Service Upgrades** pages.

What's New

Cloud Marketplace

You can now purchase a Tempered Networks cloud-based Conductor or HIPswitch directly from the Azure or Google marketplace. This greatly simplifies the purchase and deployment of Conductors and HIPswitches in your own cloud account and the setup of an independent license-ready environment.

User-Configurable LSI Prefix

You can now change the LSI prefix from 1 to another digit usage the Conductor's **Advanced Global HIPservice Settings**. This is useful if you have underlay network traffic that uses the 1.x.x.x range of addresses, which is routable on the Internet and prevalent in Asia-Pacific regions. You may choose any suitable prefix (routable or non-routable) given the distribution of your HIP Services globally. For details on routable traffic ranges, please see RFC 1918.

Android and iOS HIPclients Updated for 2.2

You can now manage Android and iOS HIPclients using the new 2.2 features, such as network objects.

Custom Overlay Policy with People Groups

People groups can be used with HIPclient and HIPserver authentication to create custom overlay network policies based on the user authenticating via the HIPclient or HIPserver. Tags specified in the people group will be added to a HIPclient or HIPserver, when a member of the people group authenticates and will be removed automatically once the session ends. The tags can be used in smart device groups to give the HIPclient or HIPserver custom overlay network policies.

Windows Client Multi-Factor Authentication (MFA)

OpenID Connect is now integrated into the Windows HIPclient and HIPserver authentication workflow. If enabled via an OpenID Connect provider, users will be required to use MFA to gain overlay access. Other HIPclient platforms will integrate client MFA for overlay access in future releases.

HIPclient and HIPserver Authentication Session Timeouts

Administrators can now configure how long a HIPclient or HIPserver authentication session will last, either globally or specific to a HIPclient or HIPserver.

Conductor Connection Failsafe

HIPswitches now have a watchdog monitor for the Conductor connection that will force a re-connect if it determines the current connection is unresponsive or missing. This should allow HIPswitches to reconnect in

More Resilient HIP Tunnels

more cases without requiring human intervention (e.g. manual rebooting or other diagnostic activities that can require physical access to the HIPswitch).

More Resilient Cellular Connectivity

HIP tunnel processes have been improved so that when a stale tunnel is detected, which may occur after reboots or carrier failures, it is rebuilt.

OSX HIPclient no longer supports El Capitan with 2.2.x

Under certain circumstances (signal strength, cell-tower location, interruptions), Verizon based HIPswitches would experience frequent modem resets resulting in an occasional failure to recover. This release has safeguards to ensure that cellular connectivity is restored after these episodes.

If you are using the mac HIPclient on El Capitan, you should not upgrade to 2.2 until you upgrade the OS.

Upgrade Considerations

We recommend that you upgrade to 2.2.2 if:

You want to use any of the following features:

- Multiple Overlays
- Multiple Underlays
- Port Groups
- Network Objects
- Automatic policy creation based on user type
- Ability to change the LSI for regional compatibility
- Windows User auth MFA

You were impacted by any issues discovered in prior releases, especially if you have any of the following:

- Cellular carrier connection issues
- Modbus GUI settings or connectivity
- HS-100 connectivity issues
- Use the 1.0.0.0/8 network address space
- Network capture on Conductor 500



Important: If you are using SHA-1 for the ESP transform, you should convert to SHA-256 before upgrading to 2.2.1.

Fixes

ID	Applies to	Description
DEV-11660	HIPswitch	A second serial port is now available for use with the SoIP feature. The Serial over IP (SoIP) feature was previously not functional on the HIPswitch 400 Series and virtual HIPSwitches. Starting in version 2.2.2, the second serial port is available for use with the SoIP feature.

ID	Applies to	Description
DEV-11631	Conductor	Fixed a firewall problem causing blocked serial connections when configured to use the Modbus communications protocol
DEV-11623	Conductor	Fixed an issue causing HIPswitches upgraded from 2.1.x while in Transparent Mode to lose their underlay network configuration, preventing them from reconnecting to the Conductor.
DEV-11596	Conductor	HIP Service online/offline alert messages now report how long they have been offline/online.
DEV-11444	Conductor	Fixed an issue where IPv4 addresses in the HIPswitch certificate conflict dialog displayed incorrectly.
DEV-11397	HIPrelay	Fixed an issue specific to the Telstra mobile network that prevented a HIPservice from connecting to its peers via a HIPrelay.
DEV-11389	Conductor	Fixed an issue where setting a HIPservice attribute rule in a Smart Device Group could prevent you from modifying HIPservice fields.
DEV-11355	Conductor	Fixed an issue where Spanning Tree Protocol was automatically enabled regardless of the previous setting during a HIPswitch upgrade.
DEV-11347	Conductor	Fixed an issue where user authentication token validation could fail if a HIPservice failed over multiple times between HA-paired Conductors.
DEV-11324	HIPswitch, Cellular	Fixed an issue where a HIPSwitch-250, or HIPswitch 150 with an NL7588 type module, could take an extended period of time to register on the Verizon network.
DEV-11318	Diagnostic mode	Changing the IP address of the Conductor no longer causes diagnostic mode to lose connection with the Conductor, however settings are no longer applied immediately. Note: You are prompted to restart the Conductor to apply the new network settings.

ID	Applies to	Description
DEV-11317	Conductor	Fixed an issue where typing in a voucher code in lowercase when provisioning a Conductor could cause errors after re-syncing with the provisioning server.
DEV-11256	Conductor	Fixed an issue where the Snort frequency and port group setting would not be set when selected for the first time.
DEV-11218	HIPclient, Android	Fixed an issue where HIPclient profile data would not be updated when the Conductor initiates a configuration change.
DEV-11184	Conductor, Hyper-V	Conductor now correctly sets the primary interface IP address to the default 192.168.56.2 on first boot.
DEV-11169	HIPswitch, Virtual	Virtual machine host time synchronization on a HIPswitch no longer produces Conductor reconnects.
DEV-11150	Conductor	The HIPswitch the customer has access to is the only one that is disabled and not the one they can not edit.
DEV-11073	Diagnostic mode	Changed the Diagnostics Port tab to display Port # instead of ETH #.
DEV-11026	BaseOS	Updated BaseOS to OpenWrt 18.06.4. The CVEs addressed by this release are listed under Security Fixes at https://openwrt.org/releases/18.06/changelog-18.06.4
DEV-10985	Conductor	Device match rules are now correctly serialized in the PCI device groups reference.
DEV-10947	Conductor	EU-north-1 region is now supported in 2.2.2.
DEV-10940	OpenHIP	TCP maximum segment size (MSS) clamping is implemented to better support traffic from clients.
DEV-10866	Conductor	Fixed an issue where you could add non-relay HIPservices to a relay HIPservice group.
DEV-10804	Conductor, PCI	The PCI log will now show details of deleted policies by default.

ID	Applies to	Description
DEV-10803	Conductor	Fixed an issue where some PCI log entry details – including firmware updates to HIPservices -- were displayed incorrectly in the user activities report.
DEV-10796	Conductor	Improved the functionality of API index filtering and sorting.
DEV-10776	Conductor	Fixed an issue where checking if a HIPservice was online triggered a HIPservice online monitor event.
DEV-10743	Conductor	The session expired message on the login page now only displays when appropriate.
DEV-10737	Conductor	You can now toggle a users network membership off after toggling it on.
DEV-10719	Conductor	Fixed an issue where opening and closing the Conductor Proxy settings could save an empty value, causing the Conductor to fail to communicate with the license server.
DEV-10701	Conductor	The port group list in the ping / traceroute drop-down will now contain each overlay port group and a single underlay option (since it is bridged) for 2.2.x HIPservices on pre 2.2 switches.

ID	Applies to	Description
DEV-10660	Conductor, Cloud	<p>Improved the route injection option to eliminate additional user actions. The new behavior is as follows:</p> <p>Route injection deletes all routes if you:</p> <ul style="list-style-type: none"> • Create a new credential provider with route injection disabled • Update the route injection option from enabled to disabled • Delete the existing credentials with route injection enabled <p>Route injection adds all routes if you:</p> <ul style="list-style-type: none"> • Create a new credential provider with route injection enabled • Update a route injection from disabled to enabled <p>Route injection will not be performed if you:</p> <ul style="list-style-type: none"> • Update credentials without changing the route injection option • Delete existing credentials with route injection disabled
DEV-10613	Conductor	Improved sorting of the Device and Device Groups pages.
DEV-10597	Conductor	Fixed an issue where cellular graphs displayed incorrect units.
DEV-10361	Diagnostic mode	Diagnostic mode should now display "None" if no part number file is found.

ID	Applies to	Description
DEV-10186	HIPshell	The Run mode shown under the <code>hipsh status</code> command now shows major operating modes first. Minor operating modes are shown in parenthesis, in gray text.
DEV-9903	Conductor, 500 Series	The Conductor 500 is now able to run packet captures.
DEV-9577	HIPclient, iOS	Fixed an issue where you needed to deny VPN requests multiple times before the correct page appeared.
DEV-9470	HIPclient, Windows	Fixed an issue where <code>hipctl profile create</code> did not create profiles successfully.
DEV-9088	Conductor	LDAP groups are now case-insensitive.
DEV-9043	Conductor	The Delete button no longer displays next to your own account on the People page.
DEV-8659	Conductor, 100 Series	Fixed an issue where the Conductor displayed an incorrect time for the HIPswitch 100g cellular.
DEV-5607	Conductor	Fixed bug where pushing large amounts of data through a HIPrelay caused the byte-count to appear as a negative number. The numbers now present as positive.

Known Issues

ID	Applies to	Description
DEV-11491	Conductor	Event Monitor of type <i>HIP tunnel</i> does not allow you to specify monitored peers. <u>Workaround:</u> None
DEV-10846	HIPclient, macOS	Currently, you cannot stop a packet capture once initiated from the Conductor UI for a macOS HIPclient. <u>Workaround:</u> Wait for the packet capture operation to terminate.

ID	Applies to	Description
DEV-10764	HIPswitch, Cellular	<p>When downgrading the HS-150 from 2.2.0 to 2.1.6, the cellular link LEDs may not be functional.</p>
		<p><u>Workaround:</u> In order to restore LED functionality, in Conductor, change the "Underlay network" settings under the "Ports" tab. For example, adjust the priority. (Note that you may need to provide the "Access point name (APN)" since that field may appear blank, in order to successfully apply the settings.) After applying the settings, reboot the HS-150 for the Cellular LEDs to become functional again.</p>
DEV-10703	Conductor	<p>If a HIPswitch is factory reset, its details may not be removed from the Conductor UI.</p>
		<p><u>Workaround:</u> none.</p>
DEV-10618	Conductor	<p>When downloading a support bundle, the dialog box contains two buttons, Download and Cancel. Cancel has the same effect as closing the dialog.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10602	HIPswitch 400, HIPswitch 500	<p>The HIPswitch 400 and HIPswitch 500 LCD menus do not support setting Conductor host names longer than 16 characters.</p>
		<p><u>Workaround:</u> Configure the corresponding IP address instead.</p>
DEV-10577	HIPshell	<p>Currently, the hipsh console will not timeout and may become locked.</p>
		<p><u>Workaround:</u> Reboot or power-cycle the HIPswitch.</p>

ID	Applies to	Description
DEV-10492	HIPrelay	<p>Once a HIPrelay learns an IPv4 / IPv6 address for a peer, it will continue to use that address indefinitely for forwarding peer packets). If the peer is offline and doesn't update its address with the HIPrelay, the old or invalid address will continue have HIP control packets forwarded to it.</p>
		<u>Workaround:</u> None
DEV-10442	Conductor	<p>In rare cases, the Apply Firmware Updates dialog will show duplicate entries in the Upgrade Available drop-down.</p>
		<u>Workaround:</u> None.
DEV-10404	OpenHIP	<p>Retransmitted HIP I1 packets are only sent using one source address/ destination pair. This differs from the initial I1 packets which attempt to use all source/destination address combinations.</p>
		<p>This issue occurs on multi-homed HIPswitches, with peer-auto connect turned on and relay probes off.</p>
		<u>Workaround:</u> None.
DEV-10276	HIPclient/HIPserver, Windows	<p>The tray application crashes repeatedly and prevents the configuration of the HIPclient or HIPserver.</p>
		<u>Workaround:</u> Reinstall .NET to resolve the issue.
DEV-10236	Conductor	<p>If you log in to multiple software HIP Services as the same user, the remote session for the first HIP Service will be terminated.</p>
		<u>Workaround:</u> None.
DEV-10200	Conductor UI	<p>Currently, users with the Network Administrator role in the Conductor can see and grant provisioning requests but are unable to view license vouchers and make top level licensing changes.</p>
		<u>Workaround:</u> None.

ID	Applies to	Description
DEV-10109	HIPclient, Windows	<p>When uninstalling the HIPclient or HIPserver, the tray icon may disappear, and the application will restart. This occurs without selecting Yes or No from the dialog.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10081	Conductor	<p>When creating a Conductor certificate using the Create Conductor Certificate dialog, you must click Save. Pressing <i>Enter</i> will result in an error and the operation will not complete successfully.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10078	Conductor	<p>Currently, HIPswitch reporting graphs do not indicate temperatures below freezing.</p>
		<p><u>Workaround:</u> None.</p>

ID	Applies to	Description
DEV-10047	HIPclient, macOS	<p>The HIPclient may lose access to the macOS keychain following an update.</p> <p><u>Workaround:</u> If this occurs, use the procedure below to resolve the issue.</p> <ol style="list-style-type: none"> 1. Open the finder by pressing Command-N 2. Find the TemperedNetworksHIP application, right click it and select Show Package Contents 3. Double-click Contents 4. Double-click MacOS 5. Keep this window available, you will need it below 6. Start Keychain Access (Applications > Utilities > Keychain Access) 7. Navigate to the System keychain (on the upper left) 8. Click on Keys (on the lower left) 9. Click on the header named Kind to sort the keys 10. For each private key with the name com.temperednetworks do the following: <ol style="list-style-type: none"> a. Double-click the item to open it b. Click Access Control c. Enter your password d. Click the + e. Drag the tnw-hipd from the window opened earlier and drop it into the window you opened by tapping + f. Click tnw-hipd, then click Add - the window will close g. Click Save Changes h. Make a note of your username, you will need this in a moment. i. Enter your password and tap Allow j. You will be prompted to enter your username and password. Do so and close the com.temperednetworks window. <p>Repeat step 10 for each private key named com.temperednetworks. You will have one key for each HIPclient profile you created.</p>

ID	Applies to	Description
DEV-9877	Conductor, Azure, wireless HIPswitch	<p>Link Manager default settings do not work between Conductors running on Azure using the Azure Network Security Group setting and wireless HIPswitches.</p>
DEV-9808	Conductor	<p>You must be a manager of every overlay that contains any device associated with all HIPservices in a HIP Service group, otherwise you lose the ability to make edits to that HIP Service group. There is no error message or any explanation as to why you are not allowed to make edits.</p>
DEV-9688	Conductor	<p>The HIPswitch Limit Bandwidthsetting currently displays as bytes per second instead of bits per second.</p>
DEV-9606	HIPswitch 150 Series	<p>When connected via serial console to a HIPswitch 150, pasting text ~35+ characters into the console requires the console to be disconnected and reconnected to restore functionality.</p>
DEV-9362	Conductor	<p>In tag properties, if you enter a month value in the Expire tag usage field, such as 1M, it is converted to weeks and days when the change is applied.</p>
DEV-8929	HIPclient, Windows	<p>After installing a windows HIPclient using the unintended install method, the tray application does not start.</p>

ID	Applies to	Description
DEV-8810	HIPswitch, Cellular	Diagnostic mode displays a drop-down menu for selecting a preferred radio access technology, however the backend does not correctly handle this setting.
		<u>Workaround:</u> None.
DEV-8806	HIPclient, HIPserver	Client authentication does not display an error message when authentication fails due to the absence of a Conductor connection.
		<u>Workaround:</u> None
DEV-8805	HIPswitch	When enabling SNAT on a HIPswitch, new connections will begin to use the overlay gateway IP address of the HIPswitch, but existing connections will not use the SNAT address until the connection is idle for the specified connection TTL or if the HIPswitch is rebooted.
		<u>Workaround:</u> Reboot the HIPswitch after enabling SNAT.
DEV-8428	Conductor, HA	The time on a standby Conductor and master conductor can become out of sync and cause missing traffic stats and health data from HIPswitches.
		<u>Workaround:</u> When failing-over an HA-paired Conductor, verify that the timestamps are the same.
DEV-8120	Conductor, Azure	In rare cases, an HIPswitch running in Azure may fail to reconnect to the Conductor after a firmware upgrade.
		<u>Workaround:</u> Restart the HIPswitch VM. Please note it can take up to 10-15 minutes to come back online.
DEV-8106	Conductor	If a device stops communicating, the Conductor UI may not reset the activity display to gray, reporting online status incorrectly.
		<u>Workaround:</u> Reload the browser.

ID	Applies to	Description
DEV-8060	Conductor	<p>In rare cases, a Conductor HA pair may stop syncing.</p> <p><u>Workaround:</u> If this occurs, promote the HA-secondary to primary, then re-pair them.</p>
DEV-7955	Conductor	<p>Pinging an Azure-hosted HIPswitch from another HIPswitch will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups.</p> <p><u>Workaround:</u> None</p>
DEV-7769	HIPswitch, Google Cloud	<p>Toggling policy too quickly on a HIPswitch running on Google Cloud can result in the route table becoming out of sync when using route injection.</p> <p><u>Workaround:</u> After toggling policy, wait 10 seconds before toggling it again.</p>
DEV-7735	HIPclient, HIPserver, All platforms	<p>HIPclients and HIPservers are currently not compatible with 1.1.1.1 DNS service.</p> <p><u>Workaround:</u> None</p>
DEV-7499	Conductor	<p>The bandwidth check in the HIPswitch Diagnostics tab may fail for HA-paired HIPswitches.</p> <p><u>Workaround:</u> None.</p>
DEV-6927	Conductor	<p>If you place a Conductor in diagnostic mode and have a non-standard port configuration defined, it may not respond to ping commands. The diagnostic mode functionality should be otherwise unaffected.</p> <p><u>Workaround:</u> None.</p>

ID	Applies to	Description
DEV-5866	HIPswitch	<p>When configuring Wi-Fi settings in diagnostic mode, the HIPswitch may override the configuration on reboot if Wi-Fi configuration was configured in the Conductor previously.</p> <p><u>Workaround:</u> Factory reset the HIPswitch before entering diagnostic mode.</p>

Release Notes 2.2.1**Release Date:** September 16 , 2019**IMPORTANT: Migrating existing Deployments to 2.2**

The 2.2 release brings a significant change to the base platform configuration and capabilities of a HIPswitch. HIPswitch versatility is dramatically increased. To achieve this, we had to give up some functional interoperability between version 2.2 and prior versions of HIP Services and Conductor. Also, Conductor 2.2 will no longer be able to manage HIP Services prior to version 2.0. While most things still work across versions 2.1.x and 2.2 during your upgrade, we recommend that 2.2.x deployments migrate completely as soon as possible using the following order:

1. Upgrade your Conductor to 2.1.6
2. Upgrade all HIP Services to 2.1.6
3. Before proceeding, ensure you have no MAP1 clients
4. Upgrade HIP Services to 2.2.1

For more information on upgrading your Conductor to 2.2.1 from prior versions, review [Conductor and HIP Service Upgrades](#).

What's New**HIP Tunnel Monitoring**

New in this release is the ability to monitor HIP tunnel state changes directly. You can configure a monitor to watch the HIP tunnel to a particular remote HIP Service or to all trusted peer HIP Services. As with all monitors, you can create actions on events to alert, change policies, etc.

HIP tunnel stats graph

The tunnel stats introduced in 2.1.5 for HIP relays is now available for all HIP Services. You can see Tx and Rx bits between any pair of HIPswitches, allowing you to troubleshoot underlay and overlay connectivity issues.

OpenID Connect

Conductors now support OpenID Connect as an external authentication provider type. You can now use an Identity and Access Management tool such as Okta or OneLogin and integrate Single Sign-On (SSO) or Multi-Factor Authentication (MFA) support.

Multiple Underlay Networks

We now support active/standby multi-homed wired and wireless uplinks, even allowing communication between different ISPs. Multiple Underlay Networks give you more control over which link handles HIP tunnels and which link handles connection to the Conductor.

Multiple Overlay Networks

We now support isolation between port groups. Each overlay port group has its own overlay IP, static routes, and related network settings. Each overlay port group bridges its interfaces, but communication between port groups requires policy.

Portgroup Configuration

The **HIPswitch > Ports** user interface has been completely overhauled to enable the configuration of multiple underlay and overlay port groups. Several things that were configured in different places in 2.1.x are now consolidated in one location:

- Port group
- Port role
- Link Manager settings
- Wi-Fi
- Cellular
- 802.1q VLAN tags
- Overlay IP/Netmask

Interfaces appear on the screen with live status information from the HIP Service. Also, all configurations are committed only after the HIP Service validates and successfully implements the changes, eliminating disagreement between what is configured in the Conductor and what is actually implemented in the HIP Service.

Network Objects

You can now use a CIDR (like 10.3.5.0/24) instead of a /32 for a device address. The term **Network Objects** simply refers to a device that uses a CIDR, and this device can be used wherever you would use any other device, like in device groups and overlay networks. Using network objects, you can allowlist an entire IP network in one click. This should make policy migration from Firewalls and Routers during new deployments much easier. Site-to-site VPN becomes trivial. More specific policies are still supported, so you can create wide policies to open general site-to-site traffic and still segment traffic to HIP Services.

Negative policies are also supported so you can allow networks or individual IP addresses (like a router) and then create exceptions using a negative policy (like a firewall).

This makes it much easier to manage HIP Services. Configurations become simpler, shorter, and easier to maintain. For cloud-based HIP Services, route injection is much simpler because routes are summarized.

User Auth (Windows, Mac, Android; iOS to release shortly)

MacOS and Android now support the user authentication feature introduced in 2.1.3 Windows clients and HIPservers. OS will support this feature in a later release. This feature allows an admin to require client users to provide an additional factor of authentication, currently username and password, to access the overlay for a period of time. Since usernames and passwords are

New shell for HIPswitches (hipsh)

centrally managed, this mitigates concerns about stolen laptops or devices, giving an admin a centrally managed way to approve and deny overlay access.

Overlay Intrusion Prevention Monitor (snort)

New in this release is **HIPshell**, a console that replaces the special login user accounts such as like *mapconfig*, *macinfo*, and *factory reset*. HIPshell provides tab-completion, inline help, and greatly expands your ability to deploy & configure a HIP Service directly without going into diagnostic mode.

HIPswitch Latency improvements

Intrusion Prevention allows you to activate any number of pre-defined rule sets. Traffic on the overlay is inspected and if a rule matches, an event is created and sent to the Conductor. You can define event actions based on Snort events.

HIP relay Performance improvements

On certain platforms with a single CPU core, the data plane latency has been reduced from 7ms to approximately 2ms. However, it is important to note that the reduction in latency can vary and depends on concurrency, packet sizes, and various other factors, but in general the latency through a HIP Service is reduced.

Full tunnel Windows clients and HIPservers

In version 2.2, we improved the speed of HIP relay traffic using XDP acceleration, allowing HIP traffic to scale even more on your existing hardware.

Multiple VLAN Tags per interface

In prior releases, a client or HIPserver needs policies to opt-in to the overlay network, the default being *split tunnel*. In version 2.2, an administrator can check a box on the client or HIPserver in the Conductor to make the default *full tunnel* and capture all network traffic into the overlay, allowing for a few exceptions that may be in the underlay like DNS, AD, etc. Please note this is Windows only; macOS clients and Linux HIPservers will be available in a future release.

MAPv1 no longer supported

We now support trunk ports, allowing you to have two or more VLANs configured on an interface. Each VLAN tag makes a new sub-interface. For example, VLAN tag 25 on eth0 creates a virtual interface named eth0.25. These interfaces can go into various port groups. East-West policies in the Conductor can be built between devices in different VLANs. Please note that you can still create bridges between VLANs as you did in version 2.1.x and earlier.

Dual-use port mode deprecated

Conductor version 2.2 and beyond will no longer be able to manage HIP Services running 2.0 and earlier. Please note that this requires you to upgrade your HIP Services to version 2.0 or later your Conductor to version 2.2. Review the upgrade section at the beginning of this document for more information about the recommended upgrade process.

Dual-use mode for interfaces is no longer available. Using multiple port groups and trunk ports, it is now much easier to implement split-tunnel with East-West policies. You can add the DNS, AD, and other servers

as protected devices to a HIP Service and give them a separate overlay port group connected to the underlay network. In Conductor, you can then give your protected devices policy to the DNS, AD, etc., servers.

Upgrade Considerations

We recommend that you upgrade to 2.2.1 if:

You want to use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following: Note: Due to the large number of changes in this release, we recommend you continue to use 2.1.x unless you need one or more of the new features described above.
<ul style="list-style-type: none"> • Multiple Overlays • Multiple Underlays • Port Groups • Network Objects 	



Important: If you are using SHA-1 for the ESP transform, you should convert to SHA-256 before upgrading to 2.2.1.



Note: You may upgrade HIPswitches to 2.2.1 provided you are running Conductor 2.2.1. Prior versions do not properly manage HIPswitch 2.2.1.

Fixes

ID	Applies to	Description
DEV-11194	Conductor	Fixed a bug where performing a Factory Reset on a HIPswitch keeps the event monitors targeted at device groups or HIP Service groups.
DEV-11144	Conductor	Fixed an issue where policy data would become out-of-sync for HIP Services that had multiple-policy connections when the remote HIP Service is revoked.
DEV-11080	Cloud	Fixed a bug where a Conductor-reboot now performs the route injection to sync the route table.
DEV-11028	Diagnostic mode	Fixed an issue where newer firmware silently failed to install from Diagnostic Mode.
DEV-10981	API	Fixed the paginated API endpoints.
DEV-10962	Conductor	Fix regression in 2.2.0 where smart device groups CIDR and IP range match rules with "only match overlay device IP" selected did not select the correct devices.

ID	Applies to	Description
DEV-10955	Conductor	<p>Fixed a bug that caused Access Point Name (APN) changes for Cellular Ports not to have any effect.</p> <p>Also APN settings from 2.1.x HIP Services will be set correctly when firmware-upgrading a HIPswitch to 2.2.</p>
DEV-10953	Diagnostic Mode	<p>The APN setting is now only configurable through the platform config under Port > Settings. This setting is available from both Diagnostic Mode and the Conductor UI.</p>
DEV-10931	HIPswitch	Included an output message informing the customer that Authentication failed.
DEV-10927	HIPswitch, Cellular	Fixed an issue that when the only active port groups are disabled, a customer will have to put the HIPswitch into Diagnostic Mode to recover it.
DEV-10913	HIPserver, Linux	Added Readme and License files and is now present on the disk.
DEV-10909	HIPswitch	Fixed a bug where the Conductor prevented the secondary HIPswitch in a HA pair from upgrading.
DEV-10905	HIPserver, Linux	A support URL was corrected for hip.service a systemd file.
DEV-10899	client/HIPserver, Windows	Fixed a bug where 'ipconfig /release', 'ipconfig /renew' - now works and NTP is able to synchronize system time DHCP broadcast is able to find DHCP server).
DEV-10898	HIPswitch-100	Fixed the ability for the HIPswitch to maintain Peers' File Information about the Peer involved in the policy.
DEV-10854	HIPswitch	When trying to configure a HS-500 and HS-400-202 in an HA pair, customers will no longer get an error the HA ports are moved to the HA portgroup. You no longer have to reboot the HIPswitch.

ID	Applies to	Description
DEV-10847	Conductor	There was an inconsistency in connectivity when a HIP Service has a device deleted from a monitored device group. HIP Service now maintains connection to the Conductor.
DEV-10826	HIPswitch	HIPswitch-250 SFP Ports 1,2,7, and 8 work at 100 and 1000 mbps speeds in 2.2.1.
DEV-10823	HIPswitch	Fixed a bug that required customers to disable Transparent Mode before attempting to enter Diagnostic Mode.
DEV-10807	Diagnostic mode	Added the Media settings back in. It now exists in the Port Configuration section. This column should only show up on a HS 250.
DEV-10797	Conductor	Fixed non-functional bandwidth check button on the Secure Tunnels Diagnostics page.
DEV-10792	HIPswitch	You are able to delete and add new DHCP server settings after configuring them.
DEV-10737	Conductor	A refresh of the browser restores proper functionality.
DEV-10726	HIPclient, macOS	Fixed the ability to uninstall the app from the About > Uninstall menu item. Additionally, you can continue to use a Command prompt: <code>sudo /Applications/TemperedNetworksHIP.app/Contents/Resources/uninstall.sh</code>
DEV-10720	Conductor, omapd	Fixed the ability to create a New Profile, a second time around, on the same Conductor.
DEV-10702	Conductor	The HIPswitch details page now displays the correct icon in the Underlay IP field, such as a Wi-Fi icon when the connection is wired.
DEV-10692	Conductor	On cell-connected HIP Services, cell details show on the Ports page as soon as they are available.
DEV-10640	HIPswitch	Able to set and maintain Conductor and Peers IP address to invisible when engaging 'Publish IPs to Conductor' to No.
DEV-10619	HIPswitch, Cellular	Fixed a USB driver issue that prevented reliable recovery from Cellular Modem Firmware crashes.

ID	Applies to	Description
DEV-10575	Conductor	Fixed a bug that could prevent users from saving Overlay DHCP settings.
DEV-10548	Conductor	Fixed a bug where, in rare cases if a monitor is invalidated, it would never try running again.
DEV-10489	API	Fixed an issue where generating a token using basic authentication for a locally authenticated user required the username to be case sensitive. This is no longer the case.
DEV-10437	Conductor	Fixed an issue where the macOS HIPclient was missing packet statistics.
DEV-10435	Conductor	Fixed an issue where importing devices using a malformed *.CSV file would stop responding and provide an incorrect error message.
DEV-10391	HIPswitch 150, Cellular	Fixed an issue where, when applying power to the HIPswitch 150, while the micro USB console port was connected to a computer, the HIPswitch would fail to enable power to the expansion bay.
DEV-10361	HIPswitch 100, HIPswitch 500	This issue is fixed for the HS 100. The diagnostic mode now display <i>None</i> if no part number file is found. This will be the case for the 100 and any other HS that does not write a part number.
DEV-10342	HIPswitch	Removed syslog-ng syntax check from init script, now syslog and udhcp start concurrently, this should allow entropy generation from network interrupts.
DEV-10356	Conductor	Fixed an issue where the + more entries link in the Edit Tags dialog would not function correctly.
DEV-10210	HIPclient/HIPserver, Windows	Upgraded to the latest versions of openssl and curl used by the Windows HIPclient and HIPserver.
DEV-10163	HIPswitch	Fixed an issue where a broadcast storm occurred when multiple HIPswitches on same L2 broadcast domain received packets from a protected device.
DEV-10136	HIPclient, macOS	The HIPclient local device ID key file permissions have been adjusted to only allow user access.

ID	Applies to	Description
DEV-10107	Conductor	Improved the error message to clearly indicate when the Conductor cannot access the licensing server.
DEV-10039	HIPswitch	Fixed an issue where HIPswitch-150 Ethernet ports would not enumerate correctly during the boot up sequence.
DEV-10023	Conductor	If you have a virtual Conductor configured with a boot drive less than 1gb in size, you will need to increase the size to 1GB or larger before Conductor version 2.2 will install. The following links provide instructions for resizing a virtual disk: <ul style="list-style-type: none">· VMware reference: https://kb.vmware.com/s/article/1004047· Hyper-V reference: https://docs.microsoft.com/en-us/powershell/module/hyper-v/resize-vhd?view=win10-ps Note: Azure, AWS, and Google Cloud Conductors already have their boot drive set to 1GB. This issue will only affect those with EXSi or Hyper-V Conductors.
DEV-9994	Conductor	Improved the error messages the Conductor adds to syslog for HIPswitches.
DEV-9993	Cloud, Google	Fixed an issue when deploying a cloud HIP Service where the Public network (VPC) drop-down would display networks with no subnets.
DEV-9922	Conductor	Cellular information now displays correctly in Ports > Underlay network .

ID	Applies to	Description
DEV-9880	OpenHIP	Fixed an issue where a HIP Service could not establish tunnels with other HIP Services if the Conductor time was adjusted to an earlier value. This could happen when enabling NTP on the Conductor for the first time.
DEV-9876	OpenHIP	Fixed an issue where HIP would crash and restart when broadcast/multicast packets were sent on a busy HIPswitch having a large number of tunnels.
DEV-9867	Conductor	Fixed an issue where HIPrelay tunnel stats were not stored in the database for HIPswitches while the tunnel was forming or disconnecting.
DEV-9845	Cloud, AWS	Fixed an issue where machine types other than t2.nano displayed incorrectly as a micro instance.
DEV-9841	Conductor	Improved the error message when creating a Cloud HIP Service and no custom images exist for the account.
DEV-9772	HIPclient, Windows	Fixed an issue where the HIPclient would not prompt for credentials if the computer was restarted.
DEV-9715	Conductor, API	The API now displays a 403 response code rather than a 401 response code when permissions for the request are incorrect or missing.
DEV-9694	Conductor, API	The API now displays correct response codes when creating endpoints.
DEV-9673	Conductor, API	When destroying endpoints, invalid IDs are now ignored.
DEV-9665	HIPswitch	Fixed an issue where health data may not be properly disabled when changing the setting from the Conductor UI.
DEV-9531	Cloud, Azure	Fixed an issue where the Image ID field would not display the correct images when the region was changed
DEV-9511	Conductor	Fixed an issue where the Forgot your password? link would not send out an email if an LDAP username was provided.
DEV-9404	Conductor, API	Removed the 406 return code from the API documentation as it is not used.

ID	Applies to	Description
DEV-9398	HIPclient, Windows	Reduced the possibility of the HIPclient tray icon remaining in the notification area when the client is terminated or uninstalled.
DEV-9392	Conductor	Fixed an issue where a HIP Service offline event may not be triggered if Check Online is used between the time a HIPswitch unexpectedly disconnects and a session timeout occurs.
DEV-9339	HIPswitch 75 Series	Resolved issues related to CPU frequency scaling on the HIPswitch 75.
DEV-9322	BaseOS	Fixed an issue where SFP ports 1 and 2 on the HIPswitch-250 did not link without 1000baseX auto-negotiation enabled on the connected switch.
DEV-9300	HIPctl	Improved the error message received when requesting a log file and it does not exist.
DEV-9159	Conductor	Fixed an issue where dropping a user who is a rule editor of a Smart Device Groups caused the group to stop functioning. The Smart Device Group will now downgrade to a standard device group to prevent possible loss of service due to permissions violations.
DEV-9157	HIPclient, macOS	Agent GUI talks to the control daemon start-up to kill existing instances of the tnw-hipd daemon that it's supposed to control.
DEV-9123	HIPswitch 250	No longer dropping packets when both the fiber and copper ports of a combo port are connected.
DEV-9122	HIPclient, macOS	Fixed an issue where setting the HIPclient Network selector to auto could result in selecting the wrong interface, if more than one was available.
DEV-9085	HIPclient, macOS	Fixed an issue that caused the control daemon to crash on shutdown.
DEV-9078	HIPclient, macOS	Fixed an issue where a support bundle could not be created support bundle due to insufficient permissions.

ID	Applies to	Description
DEV-9006	Conductor	Added more descriptive error messages due to incorrect credentials when creating cloud providers in the Conductor UI.
DEV-8804	HIPctl	Added more descriptive text to error messages received when trying to modify a profile that doesn't exist.
DEV-8633	Conductor	Regenerating an API token now requires the user to provide authentication credentials.
DEV-8561	Cloud	Added a warning message to Cloud > Diagnostics when there are no cloud provider credentials available for the HIP Service.
DEV-8529	Conductor	Currently, you cannot remove email and syslog settings in the Conductor once they are configured. <u>Workaround:</u> You can work around this issue by entering invalid values in the settings fields, click the disable button, or delete the settings using the API.
DEV-8294	Conductor	Improved syslog device_event messages to provide more useful information.
DEV-8262	Cloud, AWS, Google	Fixed an issue when deploying a HIP Service on AWS or Google Cloud where the route table was unavailable if the default region in the cloud connector was different from the HIP Service's region.
DEV-8203	Conductor	Fixed an issue in the Conductor UI where pop-up information boxes would not disappear, resulting in multiple boxes on the screen.
DEV-8202	HIPserver, Linux	Fixed an issue where a newly created profile would not be set as the default profile after completing the HIPserver installation.
DEV-8105	HIPclient, Windows	Improved the HIP Networks View to display the Overlay name instead of the ID.

ID	Applies to	Description
DEV-8085	HIPclient, HIPserver	HIPclients and HIPservers are now blocked from accepting inbound Overlay connections when an Overlay IP is not set.
DEV-8051	Conductor	Port addresses are displayed in 2.2.0.
DEV-8044	Conductor	Fixed an issue where selecting the refresh button for either cellular configurations on the Ports > Underlay network page would trigger both refresh buttons.
DEV-8012	Conductor	In rare circumstances, the traffic stat graph values can be off by a factor of 1000. If this occurs, refresh your browser.
DEV-7968	Conductor	Fixed an issue where authenticating with LDAP credentials logged the user out of the Conductor sessions.
DEV-7956	Conductor	Fixed a display issue where deleting the primary port would result in the secondary cellular interface not displaying an IP address.
DEV-7955	Conductor, Azure	If you ping an HIPswitch running Azure from another HIPswitch, the ping will now connect to the Conductor UI. This is due to ICMP being allowed by Azure's security groups.
DEV-7919	Conductor	In previous versions of the product, if a discovered device was added to a smart device group and caused an IP conflict, the device was not detected. This behavior has been improved and device will now be detected but not added to the smart device group.
DEV-7774	HIPctl	The output from hipctl has been improved. On the command line the error and status messages are now simplified for clarity, and detailed output is sent to syslog.
DEV-7720	Conductor	Fixed an issue where the + more entries link did not function correctly when selected.
DEV-7681	HIPclient, Windows	The HIPclient has been updated to improve protection against possible local threats.

ID	Applies to	Description
DEV-7661	Conductor	Fixed an issue where after replacing a HIPswitch, it could take several minutes to reconnect and appear online in the Conductor.
DEV-7507	Conductor	Upgraded our current products to support OpenSSL, version 1.1.0.
DEV-7233	Conductor	Fixed an issue where the Conductor displayed an erroneous message if the login timed-out and the user attempted to log in again without refreshing the browser.
DEV-7063	HIPclient, Windows	Added a new HIPclient control window for easier access to the HIPclient features. You can access this window by left-clicking on the tray icon.
DEV-5607	Conductor	Fixed a cosmetic issue where when pushing large amounts of data through a HIPrelay can cause the byte-count to appear as a negative number.
DEV-5713	Conductor	In rare cases, a shared network traffic graph may fail to draw data for the Conductor 400 if the 10G option card is installed. Reboot the Conductor to refresh.

Known Issues

ID	Applies to	Description
DEV-10887	HIPserver, Linux	Configuring DNS servers for a Linux HIPserver via the Conductor may not retain the settings once saved. <u>Workaround:</u> None.
DEV-10857	OpenHIP	Under certain conditions, a HIP Service may take up to 30 seconds to probe its active relays. This may result in longer initial connection delays. <u>Workaround:</u> None
DEV-10846	HIPclient, macOS	Currently, you cannot stop a packet capture once initiated from the Conductor UI for a macOS HIPclient. <u>Workaround:</u> Wait for the packet capture operation to terminate.

ID	Applies to	Description
DEV-10764	HIPswitch, Cellular	<p>When downgrading the HS-150 from 2.2.0 to 2.1.6, the cellular link LEDs may not be functional.</p>
		<p><u>Workaround:</u> In order to restore LED functionality, in Conductor, change the "Underlay network" settings under the "Ports" tab. For example, adjust the priority. (Note that you may need to provide the "Access point name (APN)" since that field may appear blank, in order to successfully apply the settings.) After applying the settings, reboot the HS-150 for the Cellular LEDs to become functional again.</p>
DEV-10703	Conductor	<p>If a HIPswitch is factory reset, its details may not be removed from the Conductor UI.</p>
		<p><u>Workaround:</u> none.</p>
DEV-10696	HIPswitch	<p>A Conductor and multi-homed HIPrelay is incompatible with 2.1.x HIPswitches and HIPclients and will cause potential connectivity issues.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10618	Conductor	<p>When downloading a support bundle, the dialog box contains two buttons, Download and Cancel. Cancel has the same effect as closing the dialog.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10602	HIPswitch 400, HIPswitch 500	<p>The HIPswitch 400 and HIPswitch 500 LCD menus do not support setting Conductor host names longer than 16 characters.</p>
		<p><u>Workaround:</u> Configure the corresponding IP address instead.</p>

ID	Applies to	Description
DEV-10592	HIPswitch, Azure	<p>If you deploy a HIPswitch using a script instead of the Conductor UI and have not configured the user credentials for the cloud provider before granting a license, it is likely you will need to reboot the HIPswitch as the route table ID will be missing in the cloud attribute.</p>
		<p><u>Workaround:</u> Deploy the HIPswitch using the Conductor UI.</p>
DEV-10577	HIPshell	<p>Currently, the hipsh console will not timeout and may become locked.</p>
		<p><u>Workaround:</u> Reboot or power-cycle the HIPswitch.</p>
DEV-10492	HIPrelay	<p>Once a HIPrelay learns an IPv4 / IPv6 address for a peer, it will continue to use that address indefinitely for forwarding peer packets). If the peer is offline and doesn't update its address with the HIPrelay, the old or invalid address will continue have HIP control packets forwarded to it.</p>
		<p><u>Workaround:</u> None</p>
DEV-10442	Conductor	<p>In rare cases, the Apply Firmware Updates dialog will show duplicate entries in the Upgrade Available drop-down.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10405	OpenHIP	<p>When sending HIP I1 packets to all peer addresses, a HIPswitch will try all source/destination address combinations and does not query the routing table. This may cause I1 packets to be sent to the wrong interface, because the source address may not match the interface address.</p>
		<p>This issue occurs on multi-homed HIPswitches, with peer-auto connect turned on and relay probes off.</p>
		<p><u>Workaround:</u> None.</p>

ID	Applies to	Description
DEV-10404	OpenHIP	<p>Retransmitted HIP I1 packets are only sent using one source address/destination pair. This differs from the initial I1 packets which attempt to use all source/destination address combinations.</p>
		<p>This issue occurs on multi-homed HIPswitches, with peer-auto connect turned on and relay probes off.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10276	HIPclient/HIPserver, Windows	<p>The tray application crashes repeatedly and prevents the configuration of the HIPclient or HIPserver.</p>
		<p><u>Workaround:</u> Reinstall .NET to resolve the issue.</p>
DEV-10236	Conductor	<p>If you log in to multiple software HIP Services as the same user, the remote session for the first HIP Service will be terminated.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10200	Conductor UI	<p>Currently, users with the Network Administrator role in the Conductor can see and grant provisioning requests but are unable to view license vouchers and make top level licensing changes.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10186	HIPshell	<p>The Run mode shown when using the <i>hipsh status</i> command may contain multiple operating modes. This is normal and not indicative of any issue.</p>
		<p><u>Workaround:</u> None.</p>
DEV-10109	HIPclient, Windows	<p>When uninstalling the HIPclient or HIPserver, the tray icon may disappear, and the application will restart. This occurs without selecting Yes or No from the dialog.</p>
		<p><u>Workaround:</u> None.</p>

ID	Applies to	Description
DEV-10081	Conductor	<p>When creating a Conductor certificate using the Create Conductor Certificate dialog, you must click Save. Pressing <i>Enter</i> will result in an error and the operation will not complete successfully.</p> <p><u>Workaround:</u> None.</p>
DEV-10078	Conductor	<p>Currently, HIPswitch reporting graphs do not indicate temperatures below freezing.</p> <p><u>Workaround:</u> None.</p>

ID	Applies to	Description
DEV-10047	HIPclient, macOS	<p>The HIPclient may lose access to the macOS keychain following an update.</p> <p>Workaround: If this occurs, use the procedure below to resolve the issue.</p> <ol style="list-style-type: none"> 1. Open the finder by pressing Command-N 2. Find the TemperedNetworksHIP application, right click it and select Show Package Contents 3. Double-click Contents 4. Double-click MacOS 5. Keep this window available, you will need it below 6. Start Keychain Access (Applications > Utilities > Keychain Access) 7. Navigate to the System keychain (on the upper left) 8. Click on Keys (on the lower left) 9. Click on the header named Kind to sort the keys 10. For each private key with the name com.temperednetworks do the following: <ol style="list-style-type: none"> a. Double-click the item to open it b. Click Access Control c. Enter your password d. Click the + e. Drag the tnw-hipd from the window opened earlier and drop it into the window you opened by tapping + f. Click tnw-hipd, then click Add - the window will close g. Click Save Changes h. Make a note of your username, you will need this in a moment i. Enter your password and tap Allow j. You will be prompted to enter your username and password. Do so and close the com.temperednetworks window. <p>Repeat step 10 for each private key named com.temperednetworks. You will have one key for each HIPclient profile you created.</p>

ID	Applies to	Description
DEV-9877	Conductor, Azure, wireless HIPswitch	<p>Link Manager default settings do not work between Conductors running on Azure using the Azure Network Security Group setting and wireless HIPswitches.</p>
		<p><u>Workaround:</u> You must Disable pings on active link on each Wireless HIPswitch or set an alternate active ping target (e.g. 8.8.8.8).</p>
DEV-9853	Diagnostic mode	<p>In diagnostic mode, if you set a static IP address using either the subnet ID or the broadcast address for a configured subnet there is no warning this setting is invalid.</p>
		<p><u>Workaround:</u> None. (Replaced by the platform configuration).</p>
DEV-9808	Conductor	<p>You must be a manager of every overlay that contains any device associated with all HIP Services in a HIP Service group, otherwise you lose the ability to make edits to that HIP Service group. There is no error message or any explanation as to why you are not allowed to make edits.</p>
		<p><u>Workaround:</u> None.</p>
DEV-9688	Conductor	<p>The HIPswitch Limit Bandwidth setting currently displays as bytes per second instead of bits per second.</p>
		<p><u>Workaround:</u> None.</p>
DEV-9606	HIPswitch 150 Series	<p>When connected via serial console to a HIPswitch 150, pasting text ~35+ characters into the console requires the console to be disconnected and reconnected to restore functionality.</p>
		<p><u>Workaround:</u> None.</p>
DEV-9362	Conductor	<p>In tag properties, if you enter a month value in the Expire tag usage field, such as 1M, it is converted to weeks and days when the change is applied.</p>
		<p><u>Workaround:</u> None</p>

ID	Applies to	Description
DEV-8929	HIPclient, Windows	<p>After installing a windows HIPclient using the unintended install method, the tray application does not start.</p>
		<p><u>Workaround:</u> Start the application manually after installation is complete</p>
DEV-8810	HIPswitch, Cellular	<p>Diagnostic mode displays a drop down menu for selecting a preferred radio access technology, however the backend does not correctly handle this setting.</p>
		<p><u>Workaround:</u> None.</p>
DEV-8805	HIPswitch	<p>When enabling SNAT on a HIPswitch, new connections will begin to use the overlay gateway IP address of the HIPswitch, but existing connections will not use the SNAT address until the connection is idle for the specified connection TTL or if the HIPswitch is rebooted.</p>
		<p><u>Workaround:</u> Reboot the HIPswitch after enabling SNAT.</p>
DEV-8428	Conductor, HA	<p>The time on a standby Conductor and master conductor can become out of sync and cause missing traffic stats and health data from HIPswitches.</p>
		<p><u>Workaround:</u> When failing-over an HA-paired Conductor, verify that the timestamps are the same.</p>
DEV-8120	Conductor, Azure	<p>In rare cases, an HIPswitch running in Azure may fail to reconnect to the Conductor after a firmware upgrade.</p>
		<p><u>Workaround:</u> Restart the HIPswitch VM. Please note it can take up to 10-15 minutes to come back online.</p>

ID	Applies to	Description
DEV-8106	Conductor	<p>If a device stops communicating, the Conductor UI may not reset the activity display to gray, reporting online status incorrectly.</p>
		<u>Workaround:</u> Reload the browser.
DEV-8060	Conductor	<p>In rare cases, a Conductor HA pair may stop syncing.</p>
		<u>Workaround:</u> If this occurs, promote the HA-secondary to primary, then re-pair them.
DEV-7769	HIPswitch, Google Cloud	<p>Toggling policy too quickly on a HIPswitch running on Google Cloud can result in the route table becoming out of sync when using route injection.</p>
		<u>Workaround:</u> After toggling policy, wait 10 seconds before toggling it again.
DEV-7499	Conductor	<p>The bandwidth check in the HIPswitch Diagnostics tab may fail for HA-paired HIPswitches.</p>
		<u>Workaround:</u> None.
DEV-6927	Conductor	<p>If you place a Conductor in diagnostic mode and have a non-standard port configuration defined, it may not respond to ping commands. The diagnostic mode functionality should be otherwise unaffected.</p>
		<u>Workaround:</u> None.
DEV-5866	HIPswitch	<p>When configuring Wi-Fi settings in diagnostic mode, the HIPswitch may override the configuration on reboot if Wi-Fi configuration was configured in the Conductor previously.</p>
		<u>Workaround:</u> Factory reset the HIPswitch before entering diagnostic mode.

Release Notes 2.1.7

Release Date: November 11, 2019

Tempered Networks has released 2.1.7 which is intended to be the last of the 2.1.x releases. This release addresses, exclusively, maintenance and stability issues for the Conductor & HIPswitch and provides enhanced security.

What's New

New in this release:

Upgrade HIPswitch and Conductor to OpenSSL 1.1

OpenSSL 1.0 goes out of support at the end of 2019. This is a proactive upgrade to the new version of the library.

Conductor Connection Failsafe

HIPswitches now have a watchdog monitor for the Conductor connection that will force a re-connect if it determines the current connection is unresponsive or missing. This should allow HIPswitches to reconnect in more cases without requiring human intervention (e.g., manual rebooting or other diagnostic activities that can require physical access to the HIPswitch).

Conductor database consistency checker

Conductors now periodically check for and repair data consistency issues. This improves the reliability of the system and should allow more issues to be resolved without human intervention.

Upgrade Considerations

The 2.1.7 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.

You may upgrade HIPswitches to 2.1.7 provided you are running Conductor 2.1.7.

We recommend you upgrade to 2.1.7 if:	
You want to take advantage of performance and stability increases in 2.1.7, or use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
<ul style="list-style-type: none"> If you have a HS that must remain on 2.1.x but work through a multi-homed 2.2.x relay. 	<ul style="list-style-type: none"> HS-100 intermittently failing to execute diagnostic commands, or appearing to upgrade but not installing the upgrade. Have intermittent issues with HS-150 cell modems Need to use the HTTP GET monitor and point it at arbitrary IP addresses Need HS-500 to not have ports 3/4, 5/6 go into hardware bypass when the unit is powered off



Note: You may upgrade Conductor directly to 2.1.7 from version 1.12.6 or later. You may upgrade HIPswitches to 2.1.7 provided you are running Conductor 2.1.7.

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.6. Additionally, 2.1.7 should be more stable than all prior releases.

Fixes

ID	Applies to	Description
DEV-11908	Conductor	Fixed an issue where viewing a HIPservice group in Diagnostic mode now refreshes the list of available HIPservices, correctly.
DEV-11863	HIPswitch-Cellular	A HIPswitch now connects via a newly installed Cell Module, when the new Cellular Module is installed after a firmware downgrade.
DEV-11182	Cloud-Azure	Microsoft Azure now supports ICMP. You are able to add ICMP rules to the Conductor and HIPswitch security groups.
DEV-11756	HIPswitch	For the HIPswitch-500 and Conductor-500 platforms: Fixed an issue where the hardware LAN bypass feature was turned on during power off. Ports 1-2, 3-4, 5-6, 7-8 were bypassed (physically connected together) when the system was powered off.
DEV-11478	HIPswitch	Fixed a bug with the Conductor-HIPswitch Time Synchronization and added a Watchdog functionality for the Conductor connection on HIPswitches.
DEV-11305	Cellular modem	Improved USB driver reliability, so Cellular Modems reliably recover from Modem Firmware crashes.
DEV-11194	Conductor	This issue is fixed where Factory resetting a HIPswitch would sometimes delete Event Monitors targeted at Device Groups or HIPservice Groups.
DEV-11047	Conductor	Added a Warning Dialog to the Conductor upgrade process if the customer has HIPswitches which are not compatible with 2.2.x.
DEV-10822	HIPswitch	Fixed a bug where entering leading zeros, in the VLAN tag input fields on the Ports Configuration page, could cause the HIPswitch to be unable to function.
DEV-10770	HIPswitch-Cellular	When downgrading a HIPswitch-150 from 2.2.0 to 2.1.6 the cellular link, LEDs are now functional.
DEV-10723	Conductor	Fixed a bug where tags were removed from HIPswitches when performing Diagnostic actions.
DEV-10696	HIPswitch	Relay probes will now probe all published addresses for a Multi-homed 2.2.x Relay. The 2.1.7 HS itself still does not support multi-homing, so probes only originate from one preferred (IPv4 or IPv6) address.
DEV-10588	Conductor	When creating a Monitor action that is an HTTP Action (HTTP GET), the URL field now allows for both the Host names and IP address.
DEV-10560	Conductor	Fixed a bug that could prevent customers from saving Overlay DHCP settings.
DEV-10390	HIPswitch-Cellular	Improved the functionality on the HIPswitch-150 and correctly applies power to the Expansion Bay on boot-up, even when the USB console cable has been connected, prior to applying main system power.
DEV-10203	HIPswitch	Fixed an issue where the default Underlay Fail-safe (reboot) settings did not get applied correctly.
DEV-10159	HIPswitch	Updated the HS-150 platform to allow multiple Underlay Interfaces (wired and cellular) to HA-pair.
DEV-9953	Conductor	A check is in place to prevent a customer from adding a HIPSwitch's Underlay IP address as a device IP for itself.

ID	Applies to	Description
DEV-9949	HIPswitch-Cellular	Enabled modem statistics collection for HIPswitch-150 with an MC7430 modem installed.
DEV-9876	OpenHIP	Fixed an issue where broadcast/multicast packets being sent on a busy HIPswitch, having many tunnels (e.g., hub with many spokes), causes the HIPswitch to crash and restart.
DEV-9830	HS100	You can now reboot a HIPSwitch from both Diagnostic Mode and the Command Line.
DEV-9829	HIPswitch	Diagnostic Mode now displays None , when there is no Part Number file.
DEV-9800	Conductor	The HIPswitch displays the tags correctly, when you toggle between Transparent Mode and Protected Mode.
DEV-9524	HIPswitch	Fixed a bug that caused Diagnostic Device pings to fail on HIPservices after an HA fail-over.
DEV-9939	Conductor	Fixed a bug where opening and closing the Conductor Proxy settings will not save blank values.

Known Issues

ID	Applies to	Description
DEV-11350	HIPapp	UserAuth sometimes does not work with 2.1.6 HIPswitches. <u>Workaround:</u> None
DEV-11095	HIPapp-Android	Android HIPclient 2.1.6 is not able to pass traffic with another HIPclient with User Authentication feature enabled. <u>Workaround:</u> Upgrade Android HIPclient to 2.2.1 or later.
DEV-11196	HIPswitch	HTTP GET monitor does not work as expected. <u>Workaround:</u> HTTP GET monitor on a 2.1.6 HS with a 2.1.7 Conductor will not work. Please upgrade the HS to 2.1.7.
DEV-11047	Conductor	A 2.1.6 Conductor with map1 HS is not blocked from upgrading to 2.2. <u>Workaround:</u> None
DEV-10638	HIPswitch	CLONE (2.1.7) - Health data is sent when it is disabled in the Conductor. <u>Workaround:</u> None
DEV-9813	Conductor	The Route Notice check does bit check the currently configured routes. <u>Workaround:</u> The UI warns that you need an Overlay Gateway Address even though one is already configured.

ID	Applies to	Description
DEV-9779	Conductor	<p>Using the mvebu image as an example, it lists the 250 variants before the 150 variants.</p> <p>The x86 image is fine.</p> <p><u>Workaround:</u> The list of platforms supported on a build image should list them in numerical order</p>
DEV-9761	Conductor	<p>The Conductor net/net utility incorrectly allows the setting of two (2) default routes.</p> <p><u>Workaround:</u> Set only one (1) default route and then apply static routes via the Setup page, under Conductor UI General Settings.</p>
DEV-9782	HIPclient, all platforms	<p>HIPclient chooses an incorrect interface and cannot establish a connection with devices behind a HIPswitch running on the Google Cloud Platform (GCP). It has to do with having multiple active interfaces.</p> <p><u>Workaround:</u> In the HIPclient configuration, select your desired network interface instead of allowing the HIPclient to automatically choose an interface.</p>
DEV-9697	Conductor	<p>Removing the Conductor HA does not remove the standby Conductor's address from the HIPswitch Conductor search list on HIPswitches running versions previous to 2.0.</p> <p><u>Workaround:</u> De-configuring Conductor HA does not remove the Standby Conductor's address from the HIPswitch Conductor search list on HIPswitch versions older than v2.0. Customer should upgrade to 2.1x.</p>
DEV-9397	Conductor	<p>If you perform a factory reset on a Conductor that's in HA-mode, the database gets into a bad state and Postgres won't start. Note that a second factory reset fixes the issue.</p> <p><u>Workaround:</u> Factory resetting a Conductor that's in an HA-pair doesn't work correctly the first time. To fix this, a second factory reset is required.</p>
DEV-9200	HIPswitch	<p>When attempting firmware upgrades get failure messages.</p> <p><u>Workaround:</u> The first attempt to upgrade fails, reboot the HS and upgrade again. (this clears out old /tmp files)</p>

ID	Applies to	Description
DEV-9166	HIPswitch, Cloud	<p>When route injection is enabled, a HIPswitch protected subnet must contain only one HIPswitch. Additionally, any custom routes added to the route table are deleted when route injection is enabled.</p> <p><u>Workaround:</u> If you want to deploy multiple HIPswitches in the same protected subnet or keep your custom routes, disable route injection.</p>
DEV-9125	HIPswitch	<p>101g: Ping peer HIPswitches pings wrong Underlay IP.</p> <p><u>Workaround:</u> On Mac and Linux HIPapp, if your computer has multiple active NICs and you select a specific NIC in HIPapp configuration, it instead lets the operating system chose the NIC for outbound traffic.</p>
DEV-8097	HIPclient, macOS	<p>If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic.</p> <p><u>Workaround:</u> None</p>
DEV-8060	Conductor	<p>In rare cases, the Conductor HA pair will stop syncing.</p> <p><u>Workaround:</u> If this happens, promote the HA-secondary to a primary, then re-pair them.</p>
DEV-8051	Conductor	<p>The IP address field on associated with a HIPswitch may be blank on the HIPservices tab.</p> <p><u>Workaround:</u> You can locate the IP address information under the Reporting tab.</p>
DEV-7769	Conductor	<p>Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the Route Table becoming out of sync when using route injection.</p> <p><u>Workaround:</u> After toggling policy, wait 10 seconds before toggling it again.</p>
DEV-7058	HIPswitch	<p>When reconfiguring your Underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings.</p> <p><u>Workaround:</u> Make the configuration changes in diagnostic mode.</p>
DEV-6590	Conductor	<p>You can add a voucher code more than once from the Licensing tab. This does not create additional licenses, but is visually confusing.</p> <p><u>Workaround:</u> None</p>
DEV-6587	Conductor	<p>The Licensing tab may display invalid entries.</p> <p><u>Workaround:</u> Remove the invalid items manually.</p>
DEV-6533	Conductor	<p>When creating or editing a smart device group, rules can have the same ordinal values. This can cause unintended issues in the processing results.</p> <p><u>Workaround:</u> When creating rules, verify each rule has a unique ordinal value.</p>

ID	Applies to	Description
DEV-6226	Conductor	A fully qualified Domain name cannot be used for local or peer replication addresses on an HA Conductor pair. <u>Workaround:</u> FQDN for Local or Peer Replication address on an HA Conductor pair can be used ONLY IF the reverse lookup yields the same FQDN
DEV-5832	HIPswitch	Device NAT functionality currently does not work with layer two (2) traffic. <u>Workaround:</u> None
DEV-5530	Conductor UI	In some cases, allow incoming pings (ICMP) and SYN Flood Protection on the Firewall page may be disabled and won't toggle. <u>Workaround:</u> Refresh your browser to resolve the issue.
DEV-5430	Conductor	After configuring the Conductor for the first time, you may receive a Lost Connection to the original server message if you select Return to settings too quickly. <u>Workaround:</u> Wait at least 20 seconds before selecting Return to settings.
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from Settings > Advanced > PCI Reporting > Downloads > User Activities Report . <u>Workaround:</u> To view names, you can download object references from the same page where you generated the PCI report.

Release Notes 2.1.6

Release Date: March 1, 2019

What's New

New in this release:

Modbus TCP to RTU Gateway

We've enhanced our Serial over IP (SoIP) feature with a Modbus TCP to Modbus RTU gateway. After configuring Modbus via the HIPswitch SoIP settings in Conductor, the HIPswitch will accept Modbus TCP commands from servers, issue the commands to serially-connected Modbus RTU device(s), and return the responses via Modbus TCP back to the server. The HIPswitch accepts pipelined requests from the server(s). This provides optimal efficiency for Modbus traffic in terms of throughput, latency, and number of messages as compared to transparent Serial over IP.

DHCP Relay

HIPswitches can now relay DHCP requests to a central DHCP server as an alternative to your existing DHCP server. This allows additional deployment flexibility where extended DHCP options are needed, or an existing DHCP server integrates with other systems such as Active Directory and DNS.



Note: When moving devices from one HIPswitch to a different one, the central DHCP server may issue the same IP address to the device, which could result in policy or routing conflicts depending on your network.

Wireless Underlay Failsafe

The HIPswitch Link Manager, introduced in version 2.1.0, intelligently monitors the health of the underlay connection, detecting when there are no options for the HIPswitch to connect to Conductor or peer HIPswitches. Link Manager is now enhanced to reboot the HIPswitch which may restore the wireless connection to a healthy state. Occasionally, changes made in the wireless provider network will drop or hang a cellular or WiFi HIPswitch uplink in such a way that the modem cannot recover. Rebooting the HS will force the modem and cell tower or access point to renegotiate their connection; sometimes this restores a healthy connection. This behavior is on by default for wireless models, and can be disabled and configured per HIPswitch in the Conductor UI. You can configure the amount of time Link Manager waits to reboot the HIPswitch after first detecting underlay failure, and a minimum amount of time to wait between reboot attempts. By default, all wireless models enable this feature with a wait-to-reboot value of 10 minutes, and min-wait-between-reboots value of 30 minutes.



Note: See known issue DEV-9877 for additional information in reference to running a HIPswitch on the Microsoft Azure platform.

APAC Modem Support

The HIPswitch cellular expansion module SFF-MOD-MC7430 (PLF-0118-01) is now available for the HIPswitch 150, which includes the Sierra Wireless MC7430 modem for operation in Hong Kong, Macau, and Japan.



Note: Firmware release 2.1.6 is required to use this expansion module.

HIPswitch 250 Series Revision 2 Support

The HIPswitch 250 Revision 2 is now available and includes the following SKUs:

- HIPswitch 250e (PLF-0062-02)
- HIPswitch 250g (PLF-0066-02)
- HIPswitch 250gd (PLF-0111-02)

Revision 2 provides improved SFP compatibility, modem watchdog support, and improved modem carrier compatibility.



Note: Firmware release 2.1.6 or higher is required to use Revision 2 of the HIPswitch 250.

Wired Interface Support for Android

The HIPclient for Android now supports wired ethernet connectivity.

Tag integration with HIP invitations

You can now specify tag(s) for HIP invitations, which apply to HIP services as they activate. This makes it

Longer HIPswitch UIDs

easy to organize newly-activated HIP services and, when combined with smart device groups, automatically give them communications policy in overlay networks.

HIPswitches which are licensed with a 2.1.6 or higher firmware may generate a longer serial number portion of the UID (up to 20 characters), compared to the previous 12 characters. HIPswitches licensed from a previous release will not change their UID.

Upgrade Considerations

The 2.1.6 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.

We recommend you upgrade to 2.1.6 if:	
You want to take advantage of performance and stability increases in 2.1.6, or use any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following:
<ul style="list-style-type: none"> • Modbus RTU to Modbus TCP proxy • HIPswitch DHCP relay • HIP invitation Tag integration • New hardware support 	<ul style="list-style-type: none"> • HIPswitch 250 cellular instability • HIPswitch 150 cellular instability • Remote Linux HIPserver HIP tunnel instability • HIPswitch 75 memory instability



Note: You may upgrade Conductor directly to 2.1.6 from version 1.12.6 or later. You may upgrade HIPswitches to 2.1.6 provided you are running Conductor 2.1.6.

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.5. Additionally, 2.1.6 should be more stable than all prior releases.

Fixes

ID	Applies to	Description
DEV-9795	HIPclient, Windows	Fixed an issue in the Windows HIPclient where a MAP connection was required for the HIPclient to begin passing traffic.
DEV-9787	HIPswitch	Fixed an issue where incorrect health data was reported while a HIPswitch was in transparent mode
DEV-9771	HIPclient, Windows	Fixed an issue where the Windows HIPclient networks view would not report all available data.
DEV-9709	HIPclient, iOS	Fixed an issue where HIPclient profiles created from HIP invites on iOS devices using the same Apple ID were synced due to iOS clipboard behavior.
DEV-9639	OpenHIP	Fixed an issue where a HIPswitch sends update acknowledgements to the wrong address.
DEV-9601	HIPclient, Android	Fixed an issue where the 2.1.5 Android HIPclient was reported incorrectly in the Conductor as version 2.1.4
DEV-9595	HIPclient, Android	After an Android device running a HIPclient wakes, ping now correctly resumes.

ID	Applies to	Description
DEV-9593	HIPclient, Android	It is no longer possible to delete the current active profile, which would cause unpredictable behavior with the HIPclient.
DEV-9574	Conductor	Fixed an issue where updating system settings after a proxy password has been entered may overwrite it with random data.
DEV-9560	HIPswitch	Fixed an issue that could cause packets on an overlay network to transmit on the underlay network under certain conditions.
DEV-9472	HIPclient, Windows	Fixed an issue with the Windows HIPclient where deleting a profile using the CLI would not update the HIPclient UI correctly, resulting in discrepancies in the profile list.
DEV-9477	Conductor	Fixed an issue in the Health Data tab where selecting more... would not display additional lines.
DEV-9389	API	POST /api/v1/people/{id}/tags in the Conductor API now presents clearer, more actionable error messages.
DEV-9382	Conductor	Improved dialog information when attempting to update firmware with an image not compatible with the target platform. The dialog text now clearly states the firmware is incorrect, replacing the generic non-actionable error message.
DEV-9385	HIPclient, Android	Fixed an issue where profile selection is disabled after creating a new profile and restarting the Android HIPclient.
DEV-9382	Conductor	Fixed an issue where attempting to install a non-Azure firmware package in an Azure instance would produce an error message stating <inserv form image> .
DEV-9377	Diagnostic mode	Fixed an issue that would allow you to enter an invalid gateway address in diagnostic mode.
DEV-9366	Cellular	Raised the log level of cellular interface repair messages to provide information about when a cellular interface is being repaired.
DEV-9333	Conductor	The Standby Conductor in an HA pair will now correctly display the Diagnostics Tab in the UI.
DEV-9317	HIPswitch	Fixed an issue where a firmware upgrade may fail due to a timing issue, taking the HIPswitch offline until it is restarted.
DEV-9312	HIPclient, Windows	Fixed an issue where an overlay IP address displayed on the Configuration settings, but not in the HIP Networks view.
DEV-9269	HIPclient, Windows	Fixed an issue where the Windows HIPclient would display an incorrect underlay IP address.
DEV-9259	Conductor	HIPclient descriptions now correctly display in the Devices Reference file from the PCI downloads page.
DEV-9201	HIPswitch 75w	Fixed an issue where the HIPswitch 75w would not properly connect to WiFi after a factory reset.
DEV-9106	HIPclient, iOS	Fixed an issue where you were required to stop and start the HIPclient to resume traffic when failing over from cellular to WiFi.
DEV-9091	HIPclient, Android	Trailing spaces are now stripped when manually entering the Conductor URL on the configuration settings.
DEV-9013	HIPswitch 75w	The WiFi LED now correctly functions on the HIPswitch 75w.

ID	Applies to	Description
DEV-7499	HIPswitch	The bandwidth check in the HIPswitch Diagnostics tab no longer fails for HA-paired HIPswitches.
DEV-6446	HIPclient, iOS	Fixed an issue where viewing traffic stats in the iOS app would display negative values instead of zero.

Known Issues

ID	Applies to	Description
DEV-9877	Conductor, Cellular HIPswitch	<p>Link Manager default settings do not work with Conductors running on the Microsoft Azure platform when using Azure Network Security Group settings.</p> <p><u>Workaround:</u> If you are using an Azure Conductor with Wireless (Cellular or WiFi) HIPswitches, disable pings on active link on each wireless HIPswitch or set an alternate active ping target (e.g. 8.8.8.8).</p>
DEV-9830	HIPswitch 100	<p>The HIPswitch 100g may sometimes fail to initiate a reboot when requested from the web interface in diagnostic mode.</p> <p><u>Workaround:</u> Power cycle the HIPswitch.</p>
DEV-9782	HIPclient, all platforms	<p>HIPclient chooses an incorrect interface and cannot establish a connection with devices behind a HIPswitch running on the Google Cloud Platform (GCP).</p> <p><u>Workaround:</u> In the HIPclient configuration, select your desired network interface instead of allowing the HIPclient to automatically choose an interface.</p>
DEV-9697	Conductor	<p>Removing Conductor HA does not remove the standby Conductor's address from the HIPswitch Conductor search list on HIPswitches running versions previous to 2.0.</p> <p><u>Workaround:</u> None</p>
DEV-9397	Conductor	<p>Factory resetting a Conductor that's in an HA-pair doesn't work correctly the first time.</p> <p><u>Workaround:</u> Factory reset the Conductor a second time to resolve the issue.</p>
DEV-9166	HIPswitch, Cloud	<p>When route injection is enabled, a HIPswitch protected subnet must contain only one HIPswitch. Additionally, any custom routes added to the route table are deleted when route injection is enabled.</p> <p><u>Workaround:</u> If you want to deploy multiple HIPswitches in the same protected subnet or keep your custom routes, disable route injection.</p>

ID	Applies to	Description
DEV-9157	HIPclient, macOS	<p>Killing the hipctl daemon (tnw-cltd) will result in the HIPclient not functioning properly.</p> <p>If you try and run any hipctl commands, the message Could not connect with Tempered Networks control process is displayed. No message is displayed when trying to make changes from the configuration UI.</p> <p><u>Workaround:</u> Restart the process by entering sudo launchctl start com.temperednetworks.ctld from a terminal.</p>
DEV-8097	HIPclient, macOS	<p>If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic.</p> <p><u>Workaround:</u> None</p>
DEV-8060	Conductor	<p>In rare cases, a Conductor HA pair will stop syncing.</p> <p><u>Workaround:</u> If this happens, promote the HA-secondary to a primary, then re-pair them.</p>
DEV-8051	Conductor	<p>The IP address field on associated with a HIPswitch may be blank on the HIPservices tab.</p> <p><u>Workaround:</u> You can locate the IP address information under the Reporting tab.</p>
DEV-7955	Conductor	<p>If you ping a HIPswitch running in Azure from another HIPswitch, it will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups.</p> <p><u>Workaround:</u> None</p>
DEV-7769	Conductor	<p>Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the route table becoming out of sync when using route injection.</p> <p><u>Workaround:</u> After toggling policy, wait 10 seconds before toggling it again.</p>
DEV-7661	Conductor	<p>When replacing a HIPswitch, the new HIPswitch may take a few minutes to reconnect and appear online in the Conductor.</p> <p><u>Workaround:</u> Wait a few minutes after replacing the HIPswitch for it to display in the Conductor UI.</p>
DEV-7125	Conductor, PCI	<p>When exporting PCI data, HIPservices references may not display correctly when viewing the CSV file in Microsoft Excel.</p> <p><u>Workaround:</u> None</p>
DEV-7058	HIPswitch	<p>When reconfiguring your underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings.</p> <p><u>Workaround:</u> Make the configuration changes in diagnostic mode.</p>

ID	Applies to	Description
DEV-6590	Conductor	You can add a voucher code more than once from the Licensing tab. This does not create additional licenses, but is visually confusing. <u>Workaround:</u> None
DEV-6587	Conductor	The Licensing tab may display invalid entries. <u>Workaround:</u> Remove the invalid items manually.
DEV-6533	Conductor	When creating or editing a smart device group, rules can have the same ordinal values. This can cause unintended issues in the processing results. <u>Workaround:</u> When creating rules, verify each rule has a unique ordinal value.
DEV-6226	Conductor	A fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair. <u>Workaround:</u> None
DEV-6195	Conductor	The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected. <u>Workaround:</u> None
DEV-5832	HIPswitch	Device NAT functionality currently does not work with layer 2 traffic. <u>Workaround:</u> None
DEV-5530	Conductor UI	In some cases, Allow incoming pings (ICMP) and SYN Flood Protection on the Firewall page may be disabled and won't toggle. <u>Workaround:</u> Refresh your browser to resolve the issue.
DEV-5430	Conductor	After configuring a Conductor for the first time, you may receive a Lost connection to the original server message if you select Return to settings too quickly. <u>Workaround:</u> Wait at least 20 seconds before selecting Return to settings.
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from Settings > Advanced > PCI Reporting > Downloads > User Activities Report . <u>Workaround:</u> To view names, you can download object references from the same page where you generated the PCI report.

Release Notes 2.1.5

Release Date: December 13, 2018

What's New

New in this release:

FIPS

Tempered Networks now offers FIPS 140-2, based on the HIPswitch 500 and Conductor 500 platforms. With FIPS, private keys are stored on the FIPS-certified HSM (hardware security module). The HSM performs all cryptographic operations. For this added key security, performance may be noticeably slower in terms of

Improved time management

data plane throughput and firmware update processing. Redundant HA FIPS is not supported at this time.

NTP sync is now configurable from the Conductor. Various improvements have been made to ensure HIPswitch time is closely synchronized with the Conductor, eliminating time-drift.



Note: We recommend pointing your HIP-enabled servers and clients to the same NTP Time source to ensure proper synchronization.

HIPswitch 75w Series

We now offer the HIPswitch 75 Series with a built-in WiFi module. Software version 2.1.5 does not currently provide WiFi LED status on the outside of the unit, but the WiFi uplink functions correctly. This will be addressed in a future release.

HIPswitch 150e Series

We now offer the HIPswitch 150e base platform, suitable for ICS and SCADA environments and includes 4x Gig-E and 1x SFP port, 1x micro-USB console port, and can be powered by PoE or external single- or dual-power supply. The HIPswitch 150 can sustain 75 Mb/s, and burst up to 100 Mb/s. This new platform supports field-upgradeable expansion modules.

HIPswitch 150 Series cellular module

This release supports a cellular expansion module suitable for North American cell carriers, which accepts 3FF Micro SIM cards. ATT, Verizon, T-Mobile, Rogers, and Telus have been field-tested at the time of this release.

HIPswitch 250 Series single- and dual-modem automated recovery

We added an internal watchdog monitor for cell carrier uplink connections. If a HIPswitch cannot connect to Conductor via any means, then occasionally (approx. once per day) it will perform a full reset, which may re-establish the carrier connection in certain environments. This will only occur when the HIPswitch 250 has no means of reaching the Conductor or peer HIPswitches.

HIPrelay bandwidth reporting

It is now possible to view the bandwidth of relayed connections between HIP Services in Conductor! An extra tab will appear in Conductor at **HIPservice > Reporting > HIPrelay Stats** for each HIPrelay. These statistics provide visibility into your network utilization with full-color, layered bandwidth graphs. They are also useful for troubleshooting underlay network relayed connection issues.

Service-specific CPU and memory reporting

For 2.1.5 and above, your HIP Services will report resource utilization more granularly, and you will be able to see this diagnostic information in the **HIPservice > Reporting > Graphs**.

Headless install for Windows HIPclient and HIPserver

You can now perform non-interactive installations of the Windows 7 HIPclient or HIPserver using Microsoft's System Center Configuration Manager (SCCM). Previous releases required manual acknowledgment by an administrator to complete the installation of an unsigned network tap (TAP) driver on Windows.

Tags public API

We have patched the driver and obtained Microsoft certification, so this step is no longer necessary.

All basic tagging capabilities released in software version 2.1.4 are exposed in the public API. This includes the ability to index the tags, set or unset tags on taggable objects, such as devices, device groups, HIP Services, HIPService groups, networks, and people. You can manage tags, retrieve various objects by tag, manage tag expirations, and perform other tag-based actions on several taggable objects at once. Advanced tag management, such as using tags in smart device group rules, or managing monitor event-actions that manipulate tags, will be added in a future release.

Custom CA alerts & public API

Though technically possible, it was difficult to use a non-Tempered CA at scale with your Conductor and HIP Services. Prior releases required you to manually copy/paste each CSR and cert from the Conductor GUI. Now you can automate the process using new public API calls. This enables a scriptable, scalable Conductor-centric workflow. Also, an admin alert is created in Conductor when custom CA certs are near expiration.

Upgrade Considerations

The 2.1.5 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.

We recommend you upgrade to 2.1.5 if:	
You want to take advantage of performance and stability increases in 2.1.5, or use any of the following features:	<p>You were impacted by any issues discovered in prior releases, especially if you have any of the following:</p> <ul style="list-style-type: none"> • Relay bandwidth reporting • HIPswitch 75w • HIPswitch 150e • HIPswitch 250gd carrier monitoring • Windows SCCM HIPclient installs • Public API for Tags or Custom CA <ul style="list-style-type: none"> • Time drift issues with Conductor or HIP Services • Cell carrier connection flapping • Issues switching cell carriers (e.g. changing SIM cards) on the HIPswitch 250 • Issues with SFP ports on the HIPswitch 250 • DHCP configuration on the overlay network • Problems setting one-arm mode on any multi-port HIPswitch • Event monitor permissions / usability problems • Difficult to detect misconfiguration problems pairing HA HIPswitches



Note: You may upgrade Conductor directly to 2.1.5 from version 1.12.6 or later. You may upgrade HIPswitches to 2.1.5 provided you are running Conductor 2.1.5.

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.4. Additionally, 2.1.5 should be more stable than all prior releases.

Fixes

ID	Applies to	Description
DEV-9462	HIPswitch	Fixed an issue with the HIPswitch 250g where ports 1, 2, and/or 7 are non-functional following an upgrade from 2.1.3 to 2.1.4, if the 100M SFP PHY setting is in use. (Otherwise it is reverting to the default of 1000M mode.)
DEV-9461	HIPswitch	Fixed an issue where port 8 on the HIPswitch 250 would not reestablish a link after a soft reboot.
DEV-9430	Conductor	The PKI tab now only displays on models that support the feature. Previously, the PKI tab was visible in the Conductor UI for HIPclients and HIPservers.
DEV-9378	HIPswitch-Cellular	Fixed an issue where cellular modems in the HIPswitch 150 and HIPswitch 250 were not properly initialized.
DEV-9370	Conductor	Fixed an issue where Conductor-initiated port configurations would fail.
DEV-9353	Conductor	All users allowed to view an alert monitor can now receive alerts for that monitor.
DEV-9333	Conductor	Fixed an issue where a standby Conductor in an HA pair would not display the Diagnostics tab.
DEV-9287	Conductor	Fixed an issue where Conductors running software version 2.1.4 sent an incorrect DHCP server configuration data to HIPswitches running versions prior to 2.1.4.
DEV-9263	HIPswitch-Cellular	Fixed an issue where a HIPswitch 250 with a cellular modem may show abnormally high CPU usage.
DEV-9246	Conductor	Attempting to delete a HIPclient or HIPserver from the Devices page no longer returns a permission denied error.
DEV-9244	HIPclient, iOS	The Conductor now correctly reports the version of the connected iOS HIPclient.
DEV-9239	Conductor	The Event Monitors view no longer prevents the Conductor UI from timing out.
DEV-9152	HIPswitch	The Conductor now rejects configuration changes that would add a 0.0.0.0 wildcard device to an overlay network if the network also has a 0.0.0.0/0 route on one of the connected HIP Services.
DEV-9149	HIPclient, Windows	The Windows HIPclient and HIPserver now report errors in the correct format.
DEV-9136	HIPserver, Linux	Fixed an issue where hipctl on Linux would not report an error when trying to reset the active profile.
DEV-9120	Conductor API	Improved the API filter and sort parameters. Sending a parameter that is not supported results in a more actionable message.
DEV-9112	Conductor	Fixed an issue where a PCI user activity report would not contain firmware upload information.

ID	Applies to	Description
DEV-9106	HIPclient, iOS	Mobile devices running iOS now failover from wireless to cellular correctly.
DEV-9053	HIPswitch	HIPswitch HA configurations now verify the HA floating IP address is in range of the shared network IP address, and will display an error in the Conductor UI if it is not.

Known Issues

ID	Applies to	Description
DEV-9887	HIPswitch 150	<p>When applying power to a HIPswitch 150 while the microUSB console port is connected to a computer, the HIPSwitch-150 fails to enable power to the expansion bay.</p> <p><u>Workaround:</u> Ensure your HIPswitch is connected to a power source prior to connecting to the console port.</p>
DEV-9875	OpenHIP	<p>When the Conductor's time is changed backwards by a large amount, such as enabling NTP on the Conductor for the first time, all connected HIPswitches will adjust their time accordingly and result in HIPswitches being unable to establish tunnels with other HIPswitches.</p> <p><u>Workaround:</u> Reboot your connected HIPswitches whenever you make large time adjustments to the Conductor.</p>
DEV-9477	Conductor	<p>The Health Data tab displays 28 lines with a link at the bottom stating +438 more. Clicking on the link does not expand the list</p> <p><u>Workaround:</u> None</p>
DEV-9397	Conductor	<p>Factory resetting a Conductor that's in an HA-pair doesn't work correctly the first time.</p> <p><u>Workaround:</u> Factory reset the Conductor a second time to resolve the issue.</p>
DEV-9382	Conductor	<p>Attempting to install a non-Azure firmware package in an Azure instance will produce an error message stating <inserv form image>.</p> <p><u>Workaround:</u> None</p>
DEV-9157	HIPclient, macOS	<p>Killing the hipctl daemon (tnw-cltd) will result in the HIPclient not functioning properly.</p> <p>If you try and run any hipctl commands, the message Could not connect with Tempered Networks control process is displayed. No message is displayed when trying to make changes from the configuration UI.</p> <p><u>Workaround:</u> Restart the process by entering sudo launchctl start com.temperednetworks.ctld from a terminal.</p>

ID	Applies to	Description
DEV-8097	HIPclient, macOS	If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic. <u>Workaround:</u> None
DEV-8060	Conductor	In rare cases, a Conductor HA pair will stop syncing. <u>Workaround:</u> If this happens, promote the HA-secondary to a primary, then re-pair them.
DEV-8051	Conductor	The IP address field on associated with a HIPswitch may be blank on the HIP Services tab. <u>Workaround:</u> You can locate the IP address information under the Reporting tab.
DEV-7955	Conductor	If you ping a HIPswitch running in Azure from another HIPswitch, it will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups. <u>Workaround:</u> None
DEV-7769	Conductor	Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the route table becoming out of sync when using route injection. <u>Workaround:</u> After toggling policy, wait 10 seconds before toggling it again.
DEV-7661	Conductor	When replacing a HIPswitch, the new HIPswitch may take a few minutes to reconnect and appear online in the Conductor. <u>Workaround:</u> Wait a few minutes after replacing the HIPswitch for it to display in the Conductor UI.
DEV-7499	HIPswitch	The bandwidth check in the HIPswitch Diagnostics tab might fail for HA-paired HIPswitches. <u>Workaround:</u> None
DEV-7125	Conductor, PCI	When exporting PCI data, HIP Services references may not display correctly when viewing the CSV file in Microsoft Excel. <u>Workaround:</u> None
DEV-7058	HIPswitch	When reconfiguring your underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings. <u>Workaround:</u> Make the configuration changes in diagnostic mode.
DEV-6590	Conductor	You can add a voucher code more than once from the Licensing tab. This does not create additional licenses, but is visually confusing. <u>Workaround:</u> None
DEV-6587	Conductor	The Licensing tab may display invalid entries. <u>Workaround:</u> Remove the invalid items manually.

ID	Applies to	Description
DEV-6533	Conductor	<p>When creating or editing a smart device group, rules can have the same ordinal values. This can cause unintended issues in the processing results.</p> <p><u>Workaround:</u> When creating rules, verify each rule has a unique ordinal value.</p>
DEV-6446	HIPclient, iOS	<p>When viewing traffic stats in the iOS app, the chart may show negative values instead of zero.</p> <p><u>Workaround:</u> None</p>
DEV-6226	Conductor	<p>A fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair.</p> <p><u>Workaround:</u> None</p>
DEV-6195	Conductor	<p>The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected.</p> <p><u>Workaround:</u> None</p>
DEV-5832	HIPswitch	<p>Device NAT functionality currently does not work with layer 2 traffic.</p> <p><u>Workaround:</u> None</p>
DEV-5530	Conductor UI	<p>In some cases, Allow incoming pings (ICMP)and SYN Flood Protection on the Firewall page may be disabled and won't toggle.</p> <p><u>Workaround:</u> Refresh your browser to resolve the issue.</p>
DEV-5430	Conductor	<p>After configuring a Conductor for the first time, you may receive a Lost connection to the original server message if you select Return to settings too quickly.</p> <p><u>Workaround:</u> Wait at least 20 seconds before selecting Return to settings.</p>
DEV-5008	PCI Reporting	<p>PCI Reporting shows the UUID reference instead of the name when generating a PCI report from Settings > Advanced > PCI Reporting > Downloads > User Activities Report.</p> <p><u>Workaround:</u> To view names, you can download object references from the same page where you generated the PCI report.</p>
DEV-1846	Conductor, HA	<p>The standby Conductor UI in an HA pair will not timeout. This issue does not affect the master Conductor UI.</p> <p><u>Workaround:</u> Log off manually when not using the standby Conductor UI.</p>

Release Notes 2.1.4

Release Date: October 16, 2018

What's New

New in this release:

HIPclient for Android

With this release, the HIPclient is available for Android. Your Android devices can now natively connect to your IDN overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different IDN overlays as needed.

Improved Conductor UI Navigation

Several UI elements have been redone to improve navigation:

- Conductor settings are now accessed from the gear icon in the upper right corner of the UI.
- The logged in user profile, API docs, EULA, and sign-out are accessed from the user account icon in the upper right corner of the UI.
- Item names in many lists throughout the UI now actively link to properties pages and dialogs. This greatly simplifies navigation between related elements.

Tags

Tags provide flexible asset management in the Conductor. Devices, Device Groups, HIPswitches, HIPswitch Groups, Overlay Networks, and People can be tagged directly. The Tag information dialog allows you to **Navigate** directly to any tagged item, perform bulk **Actions** (Enable, Disable, or Untag tagged items), and edit **Properties**. Items can be tagged permanently or until you untag them. You can also set an expiration date, which will untag a component after a configurable period of time. You can create tags from the **Tags** page, access from the tag icon in the upper right corner of the UI.

You can also create tags inline while modifying an item's tag members by entering a new tag name and select colors for easy classification. Tags have been integrated into searching and filtering throughout Conductor.

Tags can be used in matching rules to greatly simplify Smart Device Groups. They can also be added to or removed from taggable items in Event Monitor Actions, which allows monitor results to affect overlay network policies. By using tags with these features, you can optimize your workflows. For example, you can create temporary network policies for specific devices, easily revoke policy directly from devices or HIPswitches without having to navigate to a network, and allow multiple admins to keep track of their assets in a single Conductor.

Relay Probes

A HIPswitch with this option selected will periodically send probe packets to all of its relays, and use the closest relay when initiating secure tunnels. This reduces the amount of network traffic used to build new tunnels, and allows auto-connect to be turned off. You can find this option in the **Advanced settings** section of a HIPswitch's settings page.

Conductor Diagnostics

Similar to diagnostics offered for HIPswitches, the Conductor now has a set of maintenance and diagnostic functions consolidated under the Diagnostics tab of the Settings page. These include Creation or Restoration of a DB Backup, downloading a Conductor support bundle, and viewing a Conductor diagnostic report. Network diagnostics allow you to generate a packet capture on the Conductor interface, ping, and traceroute.

Upgrade Considerations

The 2.1.4 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.



Note: The Tempered Networks TERMS OF PRODUCT SALE, LICENSE AND WARRANTY has changed. The most recent version of the HIPclient for all platforms require you to accept the updated licence agreement before using the product. This applies to updates as well as new installations. For more information, see <https://www.temperednetworks.com/resources/terms-of-product-sale-license-and-warranty>

<h3>We recommend you upgrade to 2.1.4 if:</h3> <p>You want to take advantage of performance and stability increases in 2.1, especially for any of the following features:</p> <ul style="list-style-type: none"> • Android HIPclient • Improved Conductor navigation • Tags • Conductor diagnostics • Relay probes 	<p>You were impacted by any issues discovered in prior releases, especially if you have any of the following:</p> <ul style="list-style-type: none"> • If you experienced long UI start-up times in the browser (data management between the UI in the browser and the Conductor is more efficient). • Cellular connectivity and carrier selection on HIPswitch-250 models
---	--



Note: You may upgrade Conductor directly to 2.1.4 from version 1.12.6 or later. You may upgrade HIPswitches to 2.1.4 provided you are running Conductor 2.1.4.

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.3. Additionally, 2.1.4 should be more stable than all prior releases.

Enhancements

Applies to	Description
Conductor, API	Added a new node in the API, /api/v1/email_settings, containing methods for setting, updating, and retrieving Conductor email settings.
HIPclient, Windows	<p>The HIPclient for Windows has received the following improvements:</p> <ul style="list-style-type: none"> • Updated the HIPclient to allow for express installations, which requires only the license code and a confirmation. • Updated the HIPclient to allow you to set the log level in the UI.

Applies to	Description
HIPclient, macOS	<p>The HIPclient on macOS has received the following improvements:</p> <ul style="list-style-type: none"> Updated the HIPclient for to store the private key in the Keychain for newly created profiles. Updated the HIPclient for macOS to include tnw-ctld, a launch daemon on macOS for running Tempered Networks CLI commands and monitoring tnw-hipd, the HIP service. Updated the HIPclient to properly display activation code errors.
HIPclient, Windows and macOS	Updated the HIPclient UI to allow you to double-click a profile in the configuration dialog to make a profile active.
HIPswitch 500	Added support for the new 4-port 10GbE fiber-optic expansion module, available for the HIPswitch 500 Series hardware.

Fixes

ID	Applies to	Description
DEV-8849	HIPswitch	Fixed an issue on the HIPswitch 250 where using 100BASE-FX mode on port 8 could cause phantom link events.
DEV-8699	HIPclient, Linux	Fixed an issue where 32-bit platforms would drop MAP connections after a certain amount of network traffic.
DEV-8221	OpenHIP	Fixed an issue where changing the default UDP port under Settings > Advanced > Edit Settings > Host Identity Protocol Port in the Conductor was not respected by 2.1.3 HIPswitches.
DEV-8142	Conductor	Fixed an issue where clicking Finish two times very quickly when upgrading Conductor firmware would cause the upgrade to fail.
DEV-8198	Licensing	Fixed an issue where some email clients would insert additional lines in the <code>encrypted_synced_package.json</code> file and prevent the file from uploading to the Conductor correctly.
DEV-8120	HIPswitch, Azure	Fixed an issue where in rare cases, an Azure HIPswitch may fail to reconnect to the Conductor after a firmware upgrade.
DEV-8119	Conductor	Fixed an issue where a reactivated HIPclient configured with an overlay IP was listed as two devices, and you were unable to remove the overlay IP.
DEV-8067	HIPswitch	Fixed an issue that caused overlay device NAT to fail if more than one device port was used, or if the port was configured as a VLAN.
DEV-8049	Conductor	Fixed an issue where a network administrator may be able to view a HIPswitch group while restricted from viewing some of the HIPswitches in the group.
DEV-7962	HIPclient, Windows	Fixed an issue where upon waking, a computer in sleep mode would cause the HIPservice to stop and start, taking 30-60 seconds to recover.
DEV-7959	HIPswitch 100	Fixed an issue where configuring a VLAN tag on a HIPswitch 100 would cause currently active tunnels to stop working.

ID	Applies to	Description
DEV-7913	Conductor	Fixed a UI error when creating a new Cloud HIPservice where the dialog box message would display Network create completed incorrectly when the deployment creation failed.
DEV-7814	HIPclient, Windows	Fixed an issue where a user name was not retained between failed log in attempts.
DEV-6881	HIPswitch	Fixed an issue where the LCD panels on the HIPswitch 500 and Conductor 500 displayed messages incorrectly.
DEV-6507	Conductor	Fixed an issue where the throughput graph for a HIPservice would occasionally miss a data point and display it as a zero value.
DEV-6172	Conductor	Fixed an issue where a HIPclient would incorrectly show the underlay IP as the overlay IP when it did not have an overlay IP set. They now correctly display they are NAT devices in the overlay IP column.
DEV-5448	Conductor	Fixed an issue where navigating to an HA-paired secondary HIPswitch would allow you to select the Swap Roles option and cause the UI to stop responding.
DEV-5428	Conductor UI	Fixed an issue where creating a Smart Device Group with Ignore auto-discovered devices until accepted checked and then removing the setting would cause the Smart Device Group to continue ignoring unaccepted devices.
DEV-5343	Conductor UI	Fixed an issue where trying to log in after a session has timed out would generate the following error: The change you wanted was rejected.
DEV-4548	HIPswitch	HIPswitches now support 802.1p tagged traffic when using VLAN-tagged traffic in overlay networks.
DEV-4537	Conductor	Fixed an issue where the UI would not update correctly when demoting a master Conductor to standby.

Known Issues

ID	Applies to	Description
DEV-9183		
DEV-9182		
DEV-9157	HIPclient, macOS	<p>Killing the hipctl daemon (tnw-cltd) will result in the HIPclient not functioning properly.</p> <p>If you try and run any hipctl commands, the message Could not connect with Tempered Networks control process is displayed. No message is displayed when trying to make changes from the configuration UI.</p> <p><u>Workaround:</u> Restart the process by entering <code>sudo launchctl start com.temperednetworks.ctld</code> from the terminal.</p>

ID	Applies to	Description
DEV-9081	HIPclient, macOS (El Capitan)	<p>The HIPclient on macOS 10.11, El Capitan, does not provide the necessary cryptographic APIs to create and use a private key from the Keychain. Instead, the HIPclient for macOS will detect this case and store the private key in its own storage.</p> <p><u>Workaround:</u> To take advantage of the added protection using the Keychain, upgrade to macOS 10.12 (Sierra) or higher and create a new HIPclient profile.</p>
DEV-8188	HIPswitch	<p>A HIPswitch in transparent mode will not update the version information reported in the Conductor UI. This causes upgrade issues from 1.12.x to 2.x.</p> <p><u>Workaround:</u> Disable transparent mode for the HIPswitch. This updates the version information. You can then perform a firmware upgrade.</p>
DEV-8122	Conductor	<p>When creating or modifying a cloud HIPservice, the Name and Network name fields do not check for the presence of invalid characters. This will be fixed in a later release.</p> <p><u>Workaround:</u> Do not include</p> <ul style="list-style-type: none"> • Uppercase characters • Spaces • Special characters, except for a dash
DEV-8097	HIPclient, macOS	<p>If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic.</p> <p><u>Workaround:</u> None</p>
DEV-8060	Conductor	<p>In rare cases, a Conductor HA pair will stop syncing.</p> <p><u>Workaround:</u> If this happens, promote the HA-secondary to a primary, then re-pair them.</p>
DEV-8051	Conductor	<p>The IP address field associated with a HIPswitch may be blank on the HIP Services tab.</p> <p><u>Workaround:</u> You can locate the IP address information under the Reporting tab.</p>

ID	Applies to	Description
DEV-7955	Conductor	<p>If you ping a HIPswitch running in Azure from another HIPswitch, it will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups.</p> <p><u>Workaround:</u> None</p>
DEV-7814	HIPclient, Windows	<p>If user authentication fails, your user name is not retained and you must re-enter it.</p> <p><u>Workaround:</u> None</p>
DEV-7769	Conductor	<p>Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the route table becoming out of sync when using route injection.</p> <p><u>Workaround:</u> After toggling policy, wait 10 seconds before toggling it again.</p>
DEV-7661	Conductor	<p>When replacing a HIPswitch, the new HIPswitch may take a few minutes to reconnect and appear online in the Conductor.</p> <p><u>Workaround:</u> Wait a few minutes after replacing the HIPswitch for it to display in the Conductor UI.</p>
DEV-7499	HIPswitch	<p>The bandwidth check in the HIPswitch Diagnostics tab might fail for HA-paired HIPswitches.</p> <p><u>Workaround:</u> None</p>
DEV-7125	Conductor, PCI	<p>When exporting PCI data, HIP Services references may not display correctly when viewing the CSV file in Microsoft Excel.</p> <p><u>Workaround:</u> None</p>
DEV-7058	HIPswitch	<p>When reconfiguring your underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings.</p> <p><u>Workaround:</u> Make the configuration changes in diagnostic mode.</p>
DEV-6590	Conductor	<p>You can add a voucher code more than once from the Licensing tab. This does not create additional licenses, but is visually confusing. This will be fixed in a later release.</p> <p><u>Workaround:</u> None</p>
DEV-6587	Conductor	<p>The Licensing tab may display invalid entries.</p> <p><u>Workaround:</u> Remove the invalid items manually.</p>
DEV-6533	Conductor	<p>When creating or editing a smart device group, rules can have the same ordinal values. This can cause unintended issues in the processing results.</p> <p><u>Workaround:</u> When creating rules, verify each rule has a unique ordinal value.</p>
DEV-6446	HIPclient, iOS	<p>When viewing traffic stats in the iOS app, the chart may show negative values instead of zero.</p> <p><u>Workaround:</u> None</p>

ID	Applies to	Description
DEV-6226	Conductor	A fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair. <u>Workaround:</u> None
DEV-6195	Conductor	The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected. <u>Workaround:</u> None
DEV-6118	AWS	The Forgot my password link can send an invalid Conductor location. <u>Workaround:</u> Replace the location in the link with the correct Conductor address.
DEV-5832	HIPswitch	Device NAT functionality currently does not work with layer 2 traffic. <u>Workaround:</u> None
DEV-5530	Conductor UI	In some cases, Allow incoming pings (ICMP) and SYN Flood Protection on the Firewall page may be disabled and won't toggle. <u>Workaround:</u> Refresh your browser to resolve the issue.
DEV-5430	Conductor	After configuring a Conductor for the first time, you may receive a Lost connection to the original server message if you select Return to settings too quickly. <u>Workaround:</u> Wait at least 20 seconds before selecting Return to settings .
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from Settings > Advanced > PCI Reporting > Downloads > User Activities Report . <u>Workaround:</u> To view names, you can download object references from the same page where you generated the PCI report.
DEV-2417	Conductor UI	The password reset email link defaults to the first web enabled interface, and will be successful only if an administrator configures the first interface with a publicly-facing default route. <u>Workaround:</u> None.
DEV-1846	Conductor, HA	The standby Conductor UI in an HA pair will not timeout. This issue does not affect the master Conductor UI. <u>Workaround:</u> Log off manually when not using the standby Conductor UI.

Release Notes 2.1.3**Release Date:** May 24, 2018**What's New**

New in this release:

The HIPswitch 75 Series

The HIPswitch 75, released with 2.1.3, is designed for medical devices, point of sale systems, and others like building automation controls. It securely connects and protects those endpoints across all networks with little to no change to existing infrastructure. The HIPswitch 75 plug and play design makes universal connectivity and segmentation simple, fast, and cost-effective.

HIPserver for Linux

With this release, the HIPclient is now available for Linux. Your Linux devices now can natively connect to your IDN overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different IDN overlays as needed.

New platform support for Microsoft Azure and Google Cloud

You can now create, manage, and retire Microsoft Azure and Google Cloud HIP Services directly from the Conductor UI.

Support for offline Conductor licensing

We have added support to allow Conductors without access to the public Internet to complete voucher and provisioning requests with our licensing and provisioning server. You can export a sync package, send it to Tempered Networks Support, and import a file containing your licenses back in to your Conductor from a drop-down on the **Settings > Licensing** tab.

New API token system and improved token management

We have updated the API to make tokens more secure. All API requests now require two headers:

- **X-API-Client-ID** is unique by user and can be found on your user preferences page
- **X-API-Token** is generated from your user preferences page. This token is secret, so if you lose it, you must generate a new one. Whenever you refresh your token, all previous tokens will be expired.

The client ID and a refreshed secret token may also be acquired via the API using basic authorization at /api/v1/token/generate. Please refer to the API documentation for details.



Note: The **X-Person-Email** and **X-Person-Token** headers are deprecated and no longer function.

New network creation wizard

New in this release is the ability to quickly create a hub-and-spoke or full mesh network using a simple, wizard-driven UI.

Upgrade Considerations

The 2.1.3 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.



Note: You can now upgrade a HIPswitch directly to 2.1.3 from either 1.12.6 or 2.0.x. If you are running an earlier version of 1.12.x, we recommend you upgrade to 1.12.6 before upgrading to 2.1.3. When upgrading a Conductor, we recommend you upgrade to the latest stable 2.0.x first before upgrading to 2.1.3.

We recommend you upgrade to 2.1.3 if:

You want to take advantage of performance and stability increases in 2.1, especially for any of the following features:	You were impacted by any issues discovered in prior releases, especially if you have any of the following: <ul style="list-style-type: none"> • Windows HIPclient issues • macOS HIPclient issues • Cellular connectivity
---	--

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1.2. Additionally, 2.1.3 should be more stable than all prior releases.

Enhancements

Applies to	Description
Conductor	You can now run the Conductor without opening port 443 for HIPswitch communications.
High Availability	We have made performance improvements to Conductor and HIPswitch failover. Additionally, we added a progress bar during database synchronization.
HIPswitch 250e	The HIPswitch 250e now supports high-availability mode.
HIP Services	HIPswitches now support the option of setting a default route on the overlay network. This can be set on a per HIPswitch basis under the Local Devices > Overlay Routes section.
HIP Services	It is now possible to perform bulk operations on HIP Services in the Conductor UI, such as: <ul style="list-style-type: none"> • Manage • Revoke • Reactivate • Delete/Move • Check Online
HIPclient, Windows	We added additional diagnostic information in the support bundle to properly troubleshoot the HIPclient.

Applies to	Description
HIPclient, Windows	<p>The Windows HIPclient was updated to take advantage of the latest security patches.</p> <ul style="list-style-type: none"> • openssl 1.0.2o • curl 7.59.0 • JSON 10.0.3

Fixes

ID	Applies to	Description
DEV-8172	HIPswitch, Cellular	Fixed an issue where a HIPswitch 100g Verizon static IP SIM could not acquire its cellular address.
DEV-8144	HIPswitch 100g	Fixed an issue where a HIPswitch 100g modem would not correctly restart if link manager monitors failed.
DEV-8042	HIPswitch 250	Fixed an issue with the HIPswitch 250 cellular modem interface where the modem would sometimes fail to connect to the cellular network.
DEV-8017	Conductor	Fixed an issue where the Local Devices page for a HIPswitch would not display correctly after updating the properties, requiring a page refresh.
DEV-7990	HIPswitch	Fixed an issue that, would cause a HIPswitch to lose connectivity to local devices after rebooting.
DEV-7935	Conductor	Network Administrators are now able to create smart device groups.
DEV-7918	Conductor	Fixed an issue with smart device groups where negating rules that apply to CIDR/Overlay device networks returned zero device matches.
DEV-7894	HIPclient, Windows	Fixed an issue where the Windows HIPclient health data was not consistently sent to the Conductor.
DEV-7845	HIPclient, macOS	Fixed an issue where a macOS HIPclient would attempt to readdress HIP tunnels with its own overlay device IP after an address change.
DEV-7832	HIPclient, Windows	Fixed an issue where the configuration panel would not display correctly if all profiles were removed.
DEV-7746, DEV-7698	HIPswitch	Fixed an issue that caused HIPswitches to reboot when placed into diagnostic mode after being factory-reset while offline.
DEV-7699	HIPswitch 100g	Fixed an issue where changing the priority of a link may not set in a timely manner, causing problems with default routes.
DEV-7682	Conductor	Fixed an issue where importing legacy devices to the Conductor would not import device names.
DEV-7665	HIPswitch	Fixed an issue where the IMEI, IMSI, ICCID, MSISDN, and Operator ID sent to the Conductor and displayed in the HIPswitch diagnostic UI were sometimes out of date.
DEV-7608	HIPswitch	Fixed an issue where DHCP IP address changes on the underlay network could result in HIP tunnel failures.

ID	Applies to	Description
DEV-7565	HIPswitch	Fixed an issue where a HIPswitch configured in one-armed mode could cause downstream routing to local devices behind a HIPswitch to fail.
DEV-7555	HIPswitch	Fixed an issue where file transfers for support bundle requests and firmware updates would not respect the link priority after link failovers on HIPswitches.
DEV-7547	Conductor	Fixed an issue in the Conductor that prevented configuring source NAT for HIPswitches running in one-armed mode.
DEV-7531	HIPswitch	Fixed an issue where an HA pair configured to use one-arm mode could prevent it from functioning correctly.
DEV-7500	Conductor	Fixed an issue where under some circumstances device activity would not display properly in the Conductor.
DEV-7482	Conductor	Fixed an issue where the Conductor would not report a local device's MAC address or device activity if the device was configured to use NAT.
DEV-7476	Conductor	Fixed an issue where subscription licenses would not display correctly if both perpetual and subscription licenses were present for a given model.
DEV-7431	HIPclient, macOS	Fixed an issue where the configuration file for a macOS HIPclient could grow unnecessarily large after repeated configuration changes.
DEV-7379	HIPswitch	A spurious UDP packet is no longer broadcast by a HIPswitch on start-up.
DEV-7367	HIPclient, Windows	Fixed an issue where a HIPclient would fail to connect to the Conductor after being provisioned, requiring a restart.
DEV-7366	API	Fixed an issue where changes to the HIPservice settings device_auto_detect and enabled using the API would not change the settings.
DEV-7330	HIPclient, macOS	Fixed an issue where a macOS HIPclient would occasionally stop responding.
DEV-7302	HIPswitch	Fixed an issue where an upgrade of a HIPswitch in one-arm mode would rewrite port 1 MAC address to the port 2 MAC address.
DEV-7295	HIPclient, iOS	Fix an issue where an iOS HIPclient would intermittently fail to build secure connections for a newly-added device policy.
DEV-7157	Conductor	Fixed an issues where underlay traffic stats were not displayed in the Conductor if MTU was set to greater than 9000.

ID	Applies to	Description
DEV-7153	HIPswitch 400,HIPswitch 500	<p>Fixed the following issues when configuring expansion ports in diagnostic mode on the HIPswitch 500 and the HIPswitch 400 with an 8-port expansion module:</p> <ul style="list-style-type: none"> The priority field is no longer visible while the expansion port is disabled. Changing an expansion port to an underlay port now allows editing of the priority field.
DEV-7145	HIPswitch 400, HIPswitch 500	Fixed and issue where the HIPswitch 400 and HIPswitch 500 would display Manage in Conductor on the LCD display panel before being configured with a Conductor URL.
DEV-7143	HIPswitch 400, HIPswitch 500	Fixed an issue where the HIPswitch 400 and HIPswitch 500 LCD panel would continuously display Firmware Updating after applying a Hotfix from the Conductor.
DEV-7104	HIPswitch 400	Fixed an issue where placing a factory reset HIPswitch 400 in diagnostic mode before it has displayed the Manage in Conductor message on the LCD, would reboot the HIPswitch.
DEV-7092	Conductor	Fixed an issue where auto-discovered devices may display as protected devices on the Check Connectivity section of the Diagnostic tab for a HIPservice
DEV-7060	HIPswitch	Physical HIPswitch models with LCD now properly display Restarting... when rebooted from the Conductor UI, Diagnostic Mode, or the LCD.
DEV-7050	Conductor	Fixed an issue where you may receive an error accepting the EULA, when configuring a new Conductor.
DEV-7025	HIPclient, iOS	Fixed an issue where an iOS HIPclient would not allow Conductor addresses to be updated.
DEV-7014	HIPclient, Windows	HIPclient for Windows will now generate a crash dump.
DEV-6891	HIPswitch	Fixed an issue where the Conductor would not display underlay IPs in the Conductor UI if a HIPswitch was configured with multiple underlay ports.
DEV-6887	Conductor, PCI	Fixed an issue where a HIProxy rule was not added in the PCI user activities report.
DEV-6868	HIPswitch	Fixed an issue where HA-paired HIPswitches older than version 1.12.x remained offline in the Conductor after firmware-upgrading to 2.1.x.
DEV-6794	HIPswitch	Fixed an issue where remote logging would not function on HIPswitches after link failover occurred between wired and wireless connections.
DEV-6670	HIPclient, Windows	Fixed an issue where the HIPclient for Windows would not display High Availability peers correctly in network diagnostics.

ID	Applies to	Description
DEV-6563	Conductor	Fixed an issue where device group additions and removals were not captured in PCI logs.
DEV-6460	HIPclient, iOS	Fixed an issue where a HIPclient for iOS would not update its version correctly in the Conductor.
DEV-6459	Conductor	Fixed an issue where devices configured with serial-over-IP do not display in the Add devices list when attempting to add them to an overlay.
DEV-6196	HIPswitch	Fixed an issue where you were able to enter an invalid IP address without receiving an error message when configuring the Conductor URL in diagnostic mode.
DEV-6015	API	Fixed an issue in the API where the ip filter with GET /api/v1/HIP Services would return an Invalid filter parameter message.
DEV-5892	HIPswitch	Fixed an issue where a HIPswitch would go offline when using the Replace function for HIPswitches on the HIP Services tab in the Conductor UI.
DEV-5470	HIPswitch	Fixed an issues where the cellular port is missing following a factory reset of the HIPswitch.
DEV-5434	HIPswitch	Fixed an issue where clicking Detect Devices repeatedly on a HIPswitch properties page would generate excess traffic.
DEV-5089	API	Fixed an issue where some API calls would return a null string.
DEV-4944	HIPswitch	Fixed an issue where a HIPswitch may report it entered a firmware update state after installing a hotfix.
DEV-4846	HIPswitch	Fixed an issue where a HIPswitch would report it is detecting a device with the same IP as the default gateway and not display it when the HIPswitch was in one-arm mode and device discovery was on.
DEV-4357	HIPswitch-Cellular	Fixed an issue where the IMEI and MSISDN fields of a cellular modem were not displayed correctly in the Conductor and HIPswitch diagnostic UI.
DEV-4074	Conductor-SimpleConnect	Fixed an issue where the Conductor would not check if the gateway IP address is a valid IP on the overlay network when setting up an overlay DHCP server on a HIPswitch.

Known Issues

ID	Applies to	Description
DEV-8142	Conductor	If you click Finish two times very quickly when upgrading Conductor firmware, it may attempt to upgrade the Conductor twice simultaneously, causing both to fail. <u>Workaround:</u> Do not repeatedly click Finish .

ID	Applies to	Description
DEV-8122	Conductor	<p>When creating or modifying a cloud HIPservice, the Name and Network name fields do not check for the presence of invalid characters. This will be fixed in a later release.</p> <p><u>Workaround:</u> Do not include</p> <ul style="list-style-type: none"> • Uppercase characters • Spaces • Special characters, except for a dash
DEV-8120	HIPswitch, Azure	<p>In rare cases, an Azure HIPswitch may fail to reconnect to the Conductor after a firmware upgrade.</p> <p><u>Workaround:</u> In the Azure portal, restart the VM hosting the HIPswitch. It can take up to 10 or 15 minutes to come back online.</p>
DEV-8119	Conductor	<p>A reactivated HIPclient configured with an overlay IP is listed as two devices, and you are unable to remove the overlay IP.</p> <p><u>Workaround:</u> Completely delete a revoked HIPclient and allow it to come back as unmanaged in the Conductor. You can then manage it and configure as desired.</p>
DEV-8097	HIPclient, macOS	<p>If your computer has multiple active NICs and you select a specific NIC in your HIPclient configuration, the operating system will choose the NIC for outbound traffic.</p> <p><u>Workaround:</u> None</p>
DEV-8067	HIPswitch	<p>Combining NAT'd local devices and an overlay VLAN tag will block outbound overlay traffic.</p>
DEV-8060	Conductor	<p>In rare cases, a Conductor HA pair will stop syncing.</p> <p><u>Workaround:</u> If this happens, promote the HA-secondary to a primary, then re-pair them.</p>
DEV-8051	Conductor	<p>The IP address field on associated with a HIPswitch may be blank on the HIP Services tab.</p> <p><u>Workaround:</u> You can locate the IP address information under the Reporting tab.</p>

ID	Applies to	Description
DEV-8049	Conductor	<p>A network administrator may be able to view a HIPswitch group while restricted from viewing some of the HIPswitches in the group. The UI indicates the HIPswitch group is editable, but will error if modified. As a result, the user is signed out.</p> <p><u>Workaround:</u> None</p>
DEV-7962	HIPclient, Windows	<p>If your computer enters sleep mode, upon waking it may cause the HIPservice to stop and start, taking 30-60 seconds to recover.</p> <p><u>Workaround:</u> None</p>
DEV-7959	HIPswitch 100	<p>If you configures a VLAN tag on a HIPswitch 100, your currently-active tunnels may stop working.</p> <p>Workaround: To resolve this issue, perform an action that causes a HIP restart, such as:</p> <ul style="list-style-type: none"> • Reboot the HIPswitch • Change the default encryption type
DEV-7955	Conductor	<p>If you ping a HIPswitch running in Azure from another HIPswitch, it will fail in the Conductor UI. This is due to ICMP being denied by Azure's security groups.</p> <p><u>Workaround:</u> None</p>
DEV-7814	HIPclient, Windows	<p>If user authentication fails, your user name is not retained and you must re-enter it.</p> <p><u>Workaround:</u> None</p>
DEV-7769	Conductor	<p>Toggling policy on and off too quickly on a HIPswitch hosted in Google Cloud can result in the route table becoming out of sync when using route injection.</p> <p><u>Workaround:</u> After toggling policy, wait 10 seconds before toggling it again.</p>
DEV-7661	Conductor	<p>When replacing a HIPswitch, the new HIPswitch may take a few minutes to reconnect and appear online in the Conductor.</p> <p><u>Workaround:</u> Wait a few minutes after replacing the HIPswitch for it to display in the Conductor UI.</p>
DEV-7499		<p>The bandwidth check in the HIPswitch Diagnostics tab might fail for HA-paired HIPswitches.</p>
DEV-7125	PCI	<p>When exporting PCI data, HIP Services references may not display correctly when viewing the CSV file in Microsoft Excel.</p> <p><u>Workaround:</u> None</p>

ID	Applies to	Description
DEV-7058	HIPswitch	<p>When reconfiguring your underlay network from one physical port to another in the Conductor, the changes may not be applied successfully and the configuration will revert back to the original settings.</p> <p><u>Workaround:</u> Make the configuration changes in diagnostic mode.</p>
DEV-6881	HIPswitch	<p>The LCD panels in the HIPswitch 500 and Conductor-500 are 16-characters wide. Messages are currently formatted for a 20-character LCD screen and may be truncated or display on more than one line. This will be fixed in a later release.</p> <p><u>Workaround:</u> None</p>
DEV-6590	Conductor	<p>You can add a voucher code more than once from the Licensing tab. This does not create additional licenses, but is visually confusing. This will be fixed in a later release.</p> <p><u>Workaround:</u> None</p>
DEV-6587	Conductor	<p>The Licensing tab may display invalid entries.</p> <p><u>Workaround:</u> Remove the invalid items manually.</p>
DEV-6533	Conductor	<p>When creating or editing a smart device group, rules can have the same original values. This can cause unintended issues in the processing results.</p> <p><u>Workaround:</u> When creating rules, verify each rule has a unique ordinal value.</p>
DEV-6507	Conductor	<p>The throughput graph for a HIPservice may occasionally miss a data point and draws it as a zero value.</p> <p><u>Workaround:</u> Refresh the page to properly display the data point.</p>
DEV-6446	HIPclient, iOS	<p>When viewing traffic stats in the iOS app, the chart may show negative values instead of zero.</p> <p><u>Workaround:</u> None</p>
DEV-6226	Conductor	<p>Currently a fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair.</p> <p><u>Workaround:</u> None</p>
DEV-6195	Conductor	<p>The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected.</p> <p><u>Workaround:</u> None</p>
DEV-6172	Conductor	<p>When assigning a 1.x.x.x local device IP address to a HIPclient, the Conductor may continue to display the previous IP of the device.</p> <p><u>Workaround:</u> None</p>
DEV-5832	HIPswitch	<p>Device NAT functionality currently does not work with layer 2 traffic.</p> <p><u>Workaround:</u> None</p>
DEV-5530, DEV-5441	Conductor UI	<p>In some cases, Allow incoming pings (ICMP) and SYN Flood Protection on the Firewall page may be disabled and won't toggle.</p> <p><u>Workaround:</u> Refresh your browser to resolve the issue.</p>

ID	Applies to	Description
DEV-5448	Conductor UI	Clicking the Swap roles button for a secondary HA-paired HIPswitch will cause the UI to stop responding. <u>Workaround:</u> Refresh your browser.
DEV-5430	Conductor	After configuring a Conductor for the first time, you may receive a Lost connection to the original server message if you select Return to settings too quickly. <u>Workaround:</u> Wait at least 20 seconds before selecting Return to settings .
DEV-5428	Conductor UI	When you create a Smart Device Group with Ignore auto-discovered devices until accepted checked and then remove the setting, the Smart Device Group will continue to ignore unaccepted devices. <u>Workaround:</u> None
DEV-5343	Conductor UI	If you try and log in after your session has timed out, you may receive the following error: The change you wanted was rejected. <u>Workaround:</u> Refresh your browser and log in.
DEV-5008	PCI Reporting	PCI Reporting shows the UUID reference instead of the name when generating a PCI report from Settings > Advanced > PCI Reporting > Downloads > User Activities Report > . <u>Workaround:</u> To view names, you can download object references from the same page where you generated the PCI report.
DEV-4537	Conductor	When demoting a master Conductor to standby, the processing screen might not correctly update. <u>Workaround:</u> Refresh your browser.
DEV-2417	Conductor UI	The password reset email link defaults to the first web enabled interface, and will be successful only if an administrator configures the first interface with a publicly-facing default route. <u>Workaround:</u> None.
DEV-1846	Conductor, HA	Currently the standby Conductor UI in an HA pair will not timeout. This issue does not affect the master Conductor UI. <u>Workaround:</u> Log off manually when not using the standby Conductor UI.

Release Notes 2.1.2

Release Date: February 9, 2018



Important: If you are upgrading your hardware appliance to version 2.1.2 of our software, contact Tempered Networks Sales for updated licenses.

What's New

New in this release:

The HIPswitch 250 Series

The HIPswitch 250 Series is our newest hardware product and the industry's first identity-based industrial IoT gateway for Industrial Control Systems, OT, SCADA, and critical infrastructure. The HIPswitch 250 includes highly available uplinks over ethernet and up to two different cellular carriers, all actively monitored using fast failover and the ability to prioritize across both cellular and wired links. It also provides 8 x 1 Gbps and 4 x SFP (fiber or copper) with PoE, eliminating the need for ethernet switches and additional power sources. The HIPswitch 250 can also act as a HIPrelay, a feature introduced in version 2.0 of our software.

HIPclient for macOS and iOS

With this release, the HIPclient is now available for macOS and iOS. Your devices now can natively connect to your IDN overlay, giving them a trusted and verifiable connection wherever you are. Multiple profiles allow you to easily switch between different IDN overlays as needed. Additionally, integration with HIPrelay gives you seamless and secure mobility for your computers running Apple's macOS and your devices running iOS.

Link Manager

Link Manager supports all cellular platforms, including our new HIPswitch 250 Series, providing uplink redundancy and intelligent monitoring for one wired and two cellular uplinks. Dynamic switching occurs based on which port provides the best performance. Default monitors can be customized with your own destinations.

Integration with AWS

You can now create, manage, and retire AWS HIP Services directly from the Conductor UI. After creating a template, you can easily create more HIP Services to function as HIPrelays or protect virtual machines in your VPCs.

HIP Invitations

HIP Invitations, a new feature in 2.1, allow you to add mobile phones, tablets, and computers running a HIPclient or HIPserver to your IDN solution by sending the user an email containing an invitation. When the user accepts the invitation, the Conductor automatically takes care of all the steps to provision, license, manage, name, group, and create policy for the new HIPapp without manual steps by the administrator. HIPinvitations can be sent in bulk to entire organizations, and the Conductor will handle the rest.

Improved alerts and monitoring

In this release we added additional monitors, such as the **HTTP GET** monitor that allows you to parse web responses from devices in an overlay. Monitors have been expanded to support device groups and HIPservice groups. The event history graphs will now display frequently or recently triggered monitors.

Improved performance

We made significant performance improvements across the board for all platforms, with virtual HIPswitches and the HIPswitch 400 roughly doubling in performance.

Upgrade Considerations

The 2.1.2 release includes all hotfixes from prior releases and addresses all known support cases at the time of release.



Note: You can now upgrade directly to 2.1.2 from either 1.12.6 or 2.0.x. If you are running an earlier version of 1.12.x, we recommend you upgrade to 1.12.6 before upgrading to 2.1.2.



Important: You must upgrade your Conductor to the latest 2.1.2 software if you plan on using the HIPswitch 250 in your environment.

We recommend you upgrade to 2.1.2 if:	
<p>You want to take advantage of performance and stability increases in 2.1, especially for our recently added features:</p> <ul style="list-style-type: none"> • Adding our HIPswitch 250 to your environment • Increased HIPservice performance • HIPclients for additional operating systems • Simplified AWS deployments • Improved alerts and monitors 	<p>You were impacted by any issues discovered in prior releases, especially if you have any of the following:</p> <ul style="list-style-type: none"> • Stability and connectivity issues with HIP Services • Issues with the HIPswitch 200

Extensive testing was conducted both in-house and with selected development partners, in lab and in production environments to ensure that performance is equivalent to 2.1. Additionally, 2.1.2 should be more stable than all prior releases.

Enhancements

ID	Applies to	Description
DEV-5368	Conductor UI	An improved version of the import devices feature has been implemented in 2.1.
DEV-6509	Diagnostic mode	Shared network ports have been renamed to underlay ports and device ports have been renamed to local device network ports in diagnostic mode.
DEV-3427	HIPclient, Windows	Several enhancements have been made to the HIPclient for Windows: <ul style="list-style-type: none"> • Added IP/NIC/routing info, disk usage, memory usage, operating system version, and client installation version/date to event logging • Improved titles and formatting to align with other HIPservice diagnostic reports • Improved reporting so the log targets an active profile
DEV-3074	HIPclient, HIPserver	Multiple profiles have been added to the HIPclient and HIPserver, allowing multiple Conductor configurations.

Fixes

ID	Applies to	Description
DEV-7070	HIPclient, iOS	Fixed an issue where an iOS HIPclient would stop passing traffic through a HIP relay after the relay was restarted.
DEV-7064	HIPswitch, 250 Series	Fixed an issue where configuration of multiple ethernet underlay ports in diagnostic mode did not work as expected.
DEV-7061	HIPswitch, 250 Series	Fixed an issue where port 7 on the HIPswitch 250 could not be set to 100 Mbps SFP mode.
DEV-7001		Fixed an issue where multiple tunnels to a HIPservice behind a NAT through a HIP relay would fail to pass traffic when the UDP source port changed.
DEV-6767	HIPserver, Windows	Fixed an issue that caused the HIP service process to stop responding, preventing the HIPserver from restarting properly and coming back online.
DEV-6726	HIPswitch	Fixed an issue where the ping tool did not work correctly from the Tools page in diagnostic mode.
DEV-6704	Conductor	Fixed an issue where you could no longer edit the underlay port of a HIPswitch in one-arm mode if one-armed mode removed and multiple underlay network ports were configured.
DEV-6653	Conductor	Fixed an issue where a deleted HIPswitch that comes back online does not report traffic stats.
DEV-6524	HIPswitch, 400 Series	Fixed an issue where a HIPswitch 400 loses connectivity to the Conductor when configuring the HIPswitch to use one-arm mode.
DEV-6523	HIPswitch, 400 Series	Fixed an issue where changing the port configuration on a HIPswitch 400 would not revert back to its previous configuration if it was unable to contact the Conductor.
DEV-6505	Conductor	Fixed an issue where PCI reporting logs may include some passwords in the output.
DEV-6460		
DEV-6376	HIPclient, Windows	Fixed an issue where HIPclients continue to report health data at five minute intervals, regardless of changes made in the Conductor.
DEV-6309	HIPswitch	Implemented a software fix to a hardware error affecting the HIPswitch 250 front panel LEDs.
DEV-6268	Conductor	Fixed an issue where two devices in two different device groups with policy to each other would cause the connection between the HIP Services and Conductor connection to restart repeatedly.
DEV-6174	Conductor	Fixed an issue where a smart device group containing a HIPswitch group in its rules would prevent any device activated from a HIP invite to be added to the group automatically.
DEV-6073	Conductor	Fixed an issue where HIPswitch connections to Conductor would fail if network latency was greater than 500ms.
DEV-5965	Conductor	Fixed an issue where re-enabling a revoked HIPclient would not preserve its external IP address.
DEV-5891	HIPswitch	HIPswitches will now advertise their NAT underlay IP address, if set.

ID	Applies to	Description
DEV-5857	HIPswitch	A HIPswitch 200 diagnostic report does not display CPU temperature.
DEV-5541	Conductor	Fixed an issue where the Limit upload bandwidth option would disallow a packet capture on a HIPswitch until the it reboots.
DEV-5529	HIPswitch	Fixed an issue where adding an invalid overlay route to a HIPswitch from the Conductor UI would not create a route on the HIPswitch.
DEV-5526	Conductor UI	Fixed an issue where the Conductor would show devices that became active in real-time, not when active devices became inactive.
DEV-5425	BaseOS	Fixed security vulnerability CVE-2017-8890 https://nvd.nist.gov/vuln/detail/CVE-2017-8890
DEV-4558	HIPswitch, 250 Series	Fixed an issue present in that caused the multi-purpose button to not function.
DEV-3989	Conductor	Fixed an issue where you could pair HIPswitches in HA if there was no HA interface.
DEV-3619	Conductor	Fixed an issue where a recent activity email would include notifications for offline HIPclients.

Known Issues

ID	Applies to	Description
DEV-7153	HIPswitch 400,HIPswitch 500	You may experience the following issues when configuring expansion ports in diagnostic mode on the HIPswitch 500 and the HIPswitch 400 with an 8-port expansion module: <ul style="list-style-type: none"> The priority field is visible while the expansion port is disabled. Changing an expansion port to an underlay port does not enable editing of the priority field. Apply the change and then refresh your browser to allow edits to the priority field. Due to the issue above, multiple ports may temporarily have the same priority until you have finished changing the priority field, which is normally not allowed.
DEV-7157	HIPclient, Windows	Underlay traffic stats are not displayed in the Conductor if MTU is set to greater than 9000. <u>Workaround:</u> None
DEV-7145	HIPswitch 400, HIPswitch 500	The HIPswitch 400 and HIPswitch 500 may display Manage in Conductor on the LCD display panel before being configured with a Conductor URL. <u>Workaround:</u> None

ID	Applies to	Description
DEV-7143	HIPswitch 400	The HIPswitch 400 LCD panel may continuously display Firmware Updating after applying a Hotfix from the Conductor. <u>Workaround:</u> None
DEV-7125	PCI	When exporting PCI data, HIP Services references may not display correctly when viewing the CSV file in Microsoft Excel. <u>Workaround:</u> None
DEV-7092	Conductor	On the Check Connectivity section of the Diagnostic tab for a HIPservice, auto-discovered devices may display as protected devices. <u>Workaround:</u> None
DEV-7050	Conductor	When configuring a new Conductor, you may receive an error when trying to accept the EULA. <u>Workaround:</u> Change the URL in your browser to < <i>ConductorURL</i> >/app to continue.
DEV-6590	Conductor	You can add a voucher code more than once from the Licensing tab. This does not create additional licenses, but is visually confusing. This will be fixed in a later release. <u>Workaround:</u> None
DEV-6587	Conductor	The Licensing tab may display invalid entries. <u>Workaround:</u> Remove the invalid items manually.
DEV-6533	Conductor	When creating or editing a smart device group, rules can have the same original values. This can cause unintended issues in the processing results. <u>Workaround:</u> When creating rules, verify each rule has a unique ordinal value.
DEV-6507	Conductor	The throughput graph for a HIPservice may occasionally miss a data point and draws it as a zero value. <u>Workaround:</u> Refresh the page to properly display the data point.

ID	Applies to	Description
DEV-6459	Conductor	<p>Devices configured with serial-over-IP do not display in the Add devices list when attempting to add them to an overlay.</p> <p><u>Workaround:</u></p> <ol style="list-style-type: none"> 1. Create a new Smart Device Group (SDG) 2. Add a CIDR rule to the SDG and set the argument to <code>deviceIP/32</code> 3. Check only match overlay device IP 4. Click Save 5. You should now be able to sucessfully add the group containing the device to your overlay
DEV-6446	HIPclient, iOS	<p>When viewing traffic stats in the iOS app, the chart may show negative values instead of zero.</p> <p><u>Workaround:</u> None</p>
DEV-6226	Conductor	<p>Currently a fully qualified domain name cannot be used for local or peer replication addresses on an HA Conductor pair.</p> <p><u>Workaround:</u> None</p>
DEV-6196	Conductor	<p>When configuring the Conductor URL in diagnostic mode, you are able to enter an invalid IP address without receiving an error message.</p> <p><u>Workaround:</u> None</p>
DEV-6195	Conductor	<p>The Conductor incorrectly displays an option to check bandwidth for HIPclients in diagnostic view. This option is not supported for HIPclients and will not function correctly if selected.</p> <p><u>Workaround:</u> None</p>
DEV-6172	Conductor	<p>When assigning a 1.x.x.x local device IP address to a HIPclient, the Conductor may continue to display the previous IP of the device.</p> <p><u>Workaround:</u> None</p>
DEV-6130	HIPclient, Windows	<p>Setting or removing a Local Device IP on a Windows HIPclient may cause the client to report that the HIPservice is not running.</p> <p><u>Workaround:</u> Restart the HIPclient to resolve the issue.</p>
DEV-5832	HIPswitch	<p>Device NAT functionality currently does not work with layer 2 traffic.</p> <p><u>Workaround:</u> None</p>
DEV-5530, DEV-5441	Conductor UI	<p>In some cases, Allow incoming pings (ICMP) and SYN Flood Protection on the Firewall page may be disabled and won't toggle.</p> <p><u>Workaround:</u> Refresh your browser to resolve the issue.</p>

ID	Applies to	Description
DEV-5448	Conductor UI	<p>Clicking the Swap roles button for a secondary HA-paired HIPswitch will cause the UI to stop responding.</p> <p><u>Workaround:</u> Refresh your browser.</p>
DEV-5434	Conductor UI	<p>Clicking Detect Devices repeatedly on the HIPswitch properties page will generate excess traffic.</p> <p><u>Workaround:</u> Give the Conductor time to complete the operation.</p>
DEV-5430	Conductor	<p>After configuring a Conductor for the first time, you may receive a Lost connection to the original server message if you select Return to settings too quickly.</p> <p><u>Workaround:</u> Wait at least 20 seconds before selecting Return to settings.</p>
DEV-5428	Conductor UI	<p>When you create a Smart Device Group with Ignore auto-discovered devices until accepted checked and then remove the setting, the Smart Device Group will continue to ignore unaccepted devices.</p> <p><u>Workaround:</u> None</p>
DEV-5343	Conductor UI	<p>If you try and log in after your session has timed out, you may receive the following error:</p> <p>The change you wanted was rejected.</p> <p><u>Workaround:</u> Refresh your browser and log in.</p>
DEV-5008	PCI Reporting	<p>PCI Reporting shows the UUID reference instead of the name when generating a PCI report from Settings > Advanced > PCI Reporting > Downloads > User Activities Report >.</p> <p><u>Workaround:</u> To view names, you can download object references from the same page where you generated the PCI report.</p>
DEV-4846	HIPswitch	<p>If a HIPswitch is in port one-arm mode and device discovery is enabled, the HIPswitch will report an error.</p> <p><u>Workaround:</u> None</p>
DEV-4537	Conductor	<p>When demoting a master Conductor to standby, the processing screen might not correctly update.</p> <p><u>Workaround:</u> Refresh your browser.</p>
DEV-2417	Conductor UI	<p>The password reset email link defaults to the first web enabled interface, and will be successful only if an administrator configures the first interface with a publicly-facing default route.</p> <p><u>Workaround:</u> None.</p>
DEV-1846	Conductor, HA	<p>Currently the standby Conductor UI in an HA pair will not timeout. This issue does not affect the master Conductor UI.</p> <p><u>Workaround:</u> Log off manually when not using the standby Conductor UI.</p>

Release Notes for Retired Hotfixes

These hotfixes have been retired.

Release Notes 2.2.8 Hotfix – Airwall Gateway HF-2 (Retired)

Release Date: Sep 15, 2020

What's New

2.2.8 Airwall Gateway Hotfix HF-2 includes and replaces Airwall Gateway Hotfix HF-1. Once installed, it will show both HF-1 and HF-2 as installed.

This is a hotfix to release v2.2.8 for the Airwall Gateway. See [Release Notes 2.2.8](#) on page 537 for more additions in version 2.2.8. Download Airwall Gateway HF-2 from [Hotfixes](#) on page 454.



Note:

Also install Conductor HF-3, as it fixes some of these issues from the Conductor side. See [Release Notes 2.2.8 Hotfix – Conductor HF-3 \(Retired\)](#) on page 643.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you were experiencing any of the following issues:

- Blocked traffic on Airwall Gateways after installing Airwall Gateway HF-1.
- Ping devices failures.
- Airwall Gateways needing to reconnect to the Conductor.
- Airwall Gateways failing a policy check on some overlay networks

Or if you were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
DEV-14247	Airwall Gateway	Fixed a bug that was introduced in Airwall Gateway Hotfix rollup-1 that could cause traffic to get blocked on Airwall Gateways with multiple overlay port groups.
DEV-14190	Airwall Gateway	Fixed an issue that could cause traffic problems in deployments with multiple overlay port groups on the same broadcast domain.
DEV-14162	Airwall Gateway	Fixed an issue in Conductor HF-2 that was causing the "Ping devices" feature to fail for devices with plain IP addresses.
DEV-14115	Conductor	Fixed an issue that could cause infrequent Conductor service issues resulting in all Airwall Gateways needing to reconnect to the Conductor.
DEV-14067	Conductor, Airwall Gateway	Fixed an issue on 2.2.8 Airwall Edge Services that could cause false negatives in the policy check for some overlay network configurations.
DEV-13981	Airwall Gateway	Fixed an issue where setting an overlay default gateway prevented creating both the connected (local subnet) and default routes.
DEV-13974	OpenHIP	Fixed performance regression on multi-core platforms.
DEV-13926	OpenHIP	Fixed a rare packet allocation failure issue on Airwall Gateway-100.

ID	Applies to	Description
DEV-13903	Airwall Gateway	Airwall Gateway-110 models now can use the link failover monitor.
DEV-13843	Airwall Gateway	Added firewall connection states to the diagnostic report.
DEV-13275	Airwall Gateway	Fixed an issue where a misconfigured local device was corrupting the ARP cache entries for peer Airwall Gateways.

Known Issues

See [Release Notes 2.2.8](#) on page 537 for known issues.

Release Notes 2.2.8 Hotfix – Airwall Gateway HF-1 (Retired)

Release Date: Sep 3, 2020

What's New

2.2.8 Airwall Gateway Hotfix HF-1

This hotfix has been retired. These fixes are included in Airwall Gateway HF-2.

to release v2.2.8 for the Airwall Gateway. See [Release Notes 2.2.8](#) on page 537 for more additions in version 2.2.8. Download Airwall Gateway HF-1 from [Hotfixes](#) on page 454.



Note:

Also install Conductor HF-3, as it fixes some of these issues from the Conductor side. See [Release Notes 2.2.8 Hotfix – Conductor HF-3 \(Retired\)](#) on page 643.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you were experiencing any of the following issues:

- Ping devices failures.
- Airwall Gateways needing to reconnect to the Conductor.
- Airwall Gateways failing a policy check on some overlay networks

Or if you were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
DEV-14190	Airwall Gateway	Fixed an issue that could cause traffic problems in deployments with multiple overlay port groups on the same broadcast domain.
DEV-14162	Airwall Gateway	Fixed an issue in Conductor HF-2 that was causing the "Ping devices" feature to fail for devices with plain IP addresses.
DEV-14115	Conductor	Fixed an issue that could cause infrequent Conductor service issues resulting in all Airwall Gateways needing to reconnect to the Conductor.
DEV-14067	Conductor, Airwall Gateway	Fixed an issue on 2.2.8 Airwall Edge Services that could cause false negatives in the policy check for some overlay network configurations.

ID	Applies to	Description
DEV-13981	Airwall Gateway	Fixed an issue where setting an overlay default gateway prevented creating both the connected (local subnet) and default routes.
DEV-13974	OpenHIP	Fixed performance regression on multi-core platforms.
DEV-13926	OpenHIP	Fixed a rare packet allocation failure issue on Airwall Gateway-100.
DEV-13903	Airwall Gateway	Airwall Gateway-110 models now can use the link failover monitor.
DEV-13843	Airwall Gateway	Added firewall connection states to the diagnostic report.
DEV-13275	Airwall Gateway	Fixed an issue where a misconfigured local device was corrupting the ARP cache entries for peer Airwall Gateways.

Known Issues

See [Release Notes 2.2.8](#) on page 537 for known issues.

Release Notes 2.2.8 Hotfix – Conductor HF-3 (Retired)

Release Date: Sep 3, 2020

What's New

2.2.8 Conductor Hotfix HF-3

This is a hotfix to release v2.2.8 for the Conductor. This hotfix rolls up the previous Conductor hotfixes HF-1 and HF-2, so you only need to install HF-3. See [Release Notes 2.2.8](#) on page 537 for more additions in version 2.2.8. Download HF-3 from [Hotfixes](#) on page 454.



Note: Also install Airwall Gateway HF-2, as it fixes some of these issues from the Airwall Gateway side. See [Release Notes 2.2.8 Hotfix – Airwall Gateway HF-2 \(Retired\)](#) on page 641.

Upgrade Considerations

Upgrade to this 2.2.8 hotfix if you deploy Google or Alibaba Cloud Airwall Gateways from the Conductor, if you were running into the policy issues with Airwall Gateways, or were impacted by any of the other issues fixed in this hotfix.

Fixes

ID	Applies to	Description
HF-3 Fixes:		
DEV-14167	Windows Airwall Agent or Server	Fixed an issue where the Conductor was showing Windows Airwall Agents had an update available when they already had that version installed. Note that you may still see updates available for x64 Windows if you have x32 firmware downloaded on the Conductor.

ID	Applies to	Description
Includes Conductor HF-2 Fixes:		
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications of a device would delete any tags on it. Updating a device, device group, Airwall group, overlay network, or people group via the API would delete any tags on the updated object.
DEV-14080	Conductor	Fixed an issue where when adding a device directly to a device group in an Airwall Invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable policies.
DEV-14077	Conductor	Fixed an issue where the dashboard number for upgradeable Airwalls was including Airwalls that could apply an earlier version.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API.
DEV-14070	Conductor	Fixed an issue where Airwall Gateways coming online was not being included in an overlay network's Recent Activity.
DEV-14059	Conductor	Fixed an issue where you could apply HF-1 multiple times.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.
DEV-14009	Conductor	Fixed an issue where you sometimes couldn't remove static routes from an HA pair.
DEV-13944	Conductor, Airwall Gateway	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.
Includes Conductor HF-1 Fixes:		
DEV-13943	Conductor	Fixed an issue in the Tag Actions menu where devices with the tag were not included in the list of items that would be impacted by the action.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks.

ID	Applies to	Description
DEV-13930	Cloud-Alibaba, Conductor	<p>If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet.</p>
		<p>Workaround: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways.</p>
		<p>Workaround if you have already created an Alibaba Cloud Airwall Gateway:</p>
		<ol style="list-style-type: none"> 1. Apply this hotfix to your Conductor. 2. If you are not using an NTP for system time, on the Settings page, General setting tab, under System time, select Edit Settings, and then Under Update date and time, select Set browser time and then select Update. 3. For any cloud Alibaba Airwall Gateways, on the Cloud tab, Diagnostic subtab, click Refresh.
DEV-13912	Conductor	<p>Fixed an issue where secure tunnel status was not accurately reporting tunnel status for HA-paired Airwall Gateway's.</p>
DEV-13904	Cloud-Google, Conductor	<p>To deploy a 2.2.8 Google Cloud 300v Airwall Gateway from the Conductor, apply this hotfix.</p>
DEV-13893	Conductor	<p>Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, you now cannot select the Mac, Linux, or iOS platforms)</p>
DEV-13888	Conductor	<p>Fixed an issue where when you attempted to manage items from a New Airwall Online notification on the new Dashboard, it could be lost if another notice is received.</p>
DEV-13870	Conductor	<p>Fixed an issue where bandwidth would be reported multiple times, resulting in dashboard graphs reporting much higher throughput than the actual throughput.</p>
DEV-13860	Conductor	<p>Fixed an issue where when you were creating a new device, the Port affinity menu showed the first overlay port group, even though the value was set to Detect automatically.</p>

Known Issues

See [Release Notes 2.2.8](#) on page 537 for known issues.

Release Notes 2.2.8 Hotfix – Conductor HF-2 (Retired)

Release Date: Aug 19, 2020. This hotfix is included in Conductor HF-3. See [Release Notes 2.2.8 Hotfix – Conductor HF-3 \(Retired\)](#) on page 643.

Upgrade Considerations



Note: This hotfix HF-2 is included in HF-3 (see [Release Notes 2.2.8 Hotfix – Conductor HF-3 \(Retired\)](#) on page 643) and has been retired.

Fixes

ID	Applies to	Description
DEV-14103	Conductor	Fixed an issue where disabling or re-enabling network communications of a device would delete any tags on it. Updating a device, device group, Airwall group, overlay network, or people group via the API would delete any tags on the updated object.
DEV-14080	Conductor	Fixed an issue where when adding a device directly to a device group in an Airwall Invitation or during user onboarding, some of the necessary information was not being sent to the Airwall Agents and Servers to fully enable policies.
DEV-14077	Conductor	Fixed an issue where the dashboard number for upgradeable Airwalls was including Airwalls that could apply an earlier version.
DEV-14073	Conductor	Underlay IPs for 2.2.8 Airwall Gateways are now in the "underlay_ips" key in the API.
DEV-14070	Conductor	Fixed an issue where Airwall Gateways coming online was not being included in an overlay network's Recent Activity.
DEV-14067	Conductor, Airwall Gateway	Fixed an issue on 2.2.8 Airwall Gateways that could cause false negatives in the policy check for some overlay network configurations.
DEV-14059	Conductor	Fixed an issue where you could apply HF-1 multiple times.
DEV-14032	Conductor	Fixed an issue where viewing an overlay's details page in timeline view could cause an error.
DEV-14009	Conductor	Fixed an issue where you sometimes couldn't remove static routes from an HA pair.
DEV-13944	Conductor, Airwall Gateway	Fixed an issue that caused device traffic to local devices (east/west) or bypass destinations to continue after disabling the device. Traffic to remote devices was not affected.

Known Issues

See [Release Notes 2.2.8](#) on page 537 for known issues.

Release Notes 2.2.8 Hotfix – Conductor HF-1 (Retired)

Release Date: Jul 29, 2020. This Hotfix has been retired and replaced by HF-3. See [Release Notes 2.2.8 Hotfix – Conductor HF-3 \(Retired\)](#) on page 643.

Upgrade Considerations



Note: This hotfix HF-1 is included in hotfix HF-2 (retired) and HF-3 (see [Release Notes 2.2.8 Hotfix – Conductor HF-3 \(Retired\)](#) on page 643) and has been retired.

Fixes

ID	Applies to	Description
DEV-13943	Conductor	Fixed an issue in the Tag Actions menu where devices with the tag were not included in the list of items that would be impacted by the action.
DEV-13942	Conductor	People groups can now be added as managers when creating new overlay networks.
DEV-13930	Cloud-Alibaba, Conductor	If you have created a new Alibaba Cloud Airwall Gateway with v2.2.8, there is an issue with the protected subnet id on the Cloud tab actually being the public subnet. Workaround: You can avoid this issue by installing this hotfix on the Conductor before creating any Alibaba Cloud Airwall Gateways. Workaround if you have already created an Alibaba Cloud Airwall Gateway: <ol style="list-style-type: none"> 1. Apply this hotfix to your Conductor. 2. If you are not using an NTP for system time, on the Settings page, General setting tab, under System time, select Edit Settings, and then Under Update date and time, select Set browser time and then select Update. 3. For any cloud Alibaba Airwall Gateways, on the Cloud tab, Diagnostic subtab, click Refresh.
DEV-13912	Conductor	Fixed an issue where secure tunnel status was not accurately reporting tunnel status for HA-paired Airwall Gateway's.
DEV-13904	Cloud-Google, Conductor	To deploy a 2.2.8 Google Cloud 300v Airwall Gateway from the Conductor, apply this hotfix.
DEV-13893	Conductor	Fixed an issue where you could select Airwall Edge Services that do not support health data for the health data monitor (for example, you now cannot select the Mac, Linux, or iOS platforms)
DEV-13888	Conductor	Fixed an issue where when you attempted to manage items from a New Airwall Online notification on the new Dashboard, it could be lost if another notice is received.
DEV-13870	Conductor	Fixed an issue where bandwidth would be reported multiple times, resulting in dashboard graphs reporting much higher throughput than the actual throughput.
DEV-13860Th	Conductor	Fixed an issue where when you were creating a new device, the Port affinity menu showed the first overlay port group, even though the value was set to Detect automatically .

Known Issues

See [Release Notes 2.2.8](#) on page 537 for known issues.

Get Support

You can often find answers to your questions in Airwall helpthe guide, or by searching knowledge base articles on the Customer Success site: <https://tempered.force.com/TemperedSupportCenter/s/>.

If you still cannot find what you are looking for, you can Customer Success at support@tempered.io for help.

How to get support

You can often find answers to your questions in Airwall helpthe guide, or by logging in to your **Support** account and searching the knowledge base articles. If you still cannot find what you are looking for, you can contact support for help.



Note: You must have a current support contract with Tempered to open a support ticket.

There are several ways to contact support.

Open a case on the Tempered Support Web Portal

1. Go to <https://www.tempered.io/support/supportReq.html>.
2. Sign in using your support account log in.
3. Click + or **New**.
4. Fill in the name and contact information.
5. Provide the **Information to Include** listed below.
6. Attach the support bundle from the affected devices.
7. For network issues, attach a packet capture.

Contact Tempered Support via email

1. Send an email message to support@tempered.io.
2. Provide the **Information to Include** listed below.
3. Attach your support bundle to the email.
4. For network issues, attach a packet capture.

Information to Include

Provide the following information when you open a case with Tempered Support:

- A full description of the issue, including the following details:
 - The symptoms of the issue, including a brief description of all systems applicable to the configuration.
 - The approximate time the issue first occurred.
 - The number of times the issue has recurred.
 - Any error output provided by the system.
 - Steps to reproduce the issue.
 - Any changes you made to the system close to when the issue first occurred.
 - Any steps you've taken to resolve the issue.
 - Whether this is a new implementation.
 - How many data centers and devices are applicable to the configuration.
 - Which devices are affected by the issue.

- A description of the impact the issue is having on your site.
- Days and times you are available to work on the issue, and any alternative contacts that can work on the issue if you are not available.

Get a Support Bundle

The Support Bundle is the technical information about the device. To best answer support issues, Tempered Support needs the Support Bundle from the Conductor and Support Bundles from any Airwall Gateway, Airwall Agent, and/or Airwall Server that is part of the issue you are reporting. For more assistance, see [Create a support bundle from the Conductor](#) on page 412.

Get a Packet capture

If the issue involves the network, perform a packet capture while the issue is occurring. Provide this packet capture when you open the case. For more assistance, see [Troubleshoot an Airwall Gateway by using packet capture](#) on page 415.

Documentation Downloads

You can print PDF copies of any topic by clicking the print icon  at the top right of any topic.

Download the most recent PDF of Airwall help:

[Airwall help](#)

[Download latest](#) Includes 2.2.11 - created Mar 15, 2021

Go here for [Pre-Airwall Documentation Downloads](#).



Tip: Select a Blue button below to download a manual in PDF format. Documentation downloads are organized by product version.

User Manuals

Conductor and Airwall Edge Services Administrator Guide

This document contains procedural information help you understand how to install, configure, and manage your Conductor, Airwall Edge Services, devices, and protected networks.

[Download for 2.1](#)

Conductor and Airwall Edge Services Install Guide

This document outlines the steps required to deploy a Conductor, connect Airwall Edge Services, add devices, create and manage an overlay, and configure device trust.



Note: The contents of the **Install Guide** are also included in the **Administrator Guide**. Use this guide if you need a shorter document consisting of basic instructions about installing and configuring your Conductor and Airwall Edge Services.

[Download for 2.1](#)

Airwall Agent and Airwall Server Quick Start Guide

This document contains procedural information help you understand how to install, configure, and manage Airwall Agents and Airwall Servers.

[Download for 2.1](#)

Documentation for Cloud Platforms

You can create and manage your Conductors and Airwall Edge Services in Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). The guides listed below provide end-to-end instructions on various aspects of your cloud deployment.

Deploy an Airwall Edge Service on the Amazon Web Services Platform

This document outlines the steps required to deploy an Airwall Edge Service on AWS.

[Download for 2.1](#)

Deploy a Conductor on Microsoft Azure

This document outlines the steps required to deploy a Conductor on Azure.

[Download for 2.1](#)

Deploy a Conductor on the Google Cloud Platform

This document outlines the steps required to deploy a Conductor on GCP.

[Download for 2.1](#)

Hardware Specification Sheets and Platform Guides

If you no longer have access to the documentation included with your hardware, you can download a PDF here.



Tip: Search your model number in help for updated versions.

Airwall Gateway 110e and 110g

[Airwall Gateway 110 Quick Start and Platform Guide](#)

Airwall Gateway/HIPswitch 75e

[Airwall Gateway/HIPswitch 75 Series Quick Start Guide](#)



Note: See [Serial drivers](#) on page 445 and install the serial driver if you want to use the serial port on the 75.

Airwall Gateway/HIPswitch 100e and 100g

[Airwall Gateway 100 Series Platform Guide](#)

Airwall Gateway/HIPswitch 150 and I-150

[Airwall Gateway 150 Series Platform Guide](#)

[Airwall Gateway 150 Series Hardware Specifications sheet](#)

[Airwall Gateway 150 Expansion Module Manual](#)

Airwall Gateway/HIPswitch 150 Series - Expansion Modules (SFF-MOD-NL7588 and SFF-MOD-MC7430 cellular expansion modules)

[Airwall Gateway 250 Platform Guide](#)



Note: See [Serial drivers](#) on page 445 and install the serial driver if you want to use the serial port on the 250.

[Airwall Gateway/HIPswitch 400 Series Platform Guide](#)

[Conductor or Airwall Gateway 500 Platform Guide](#)

[Airwall Gateway 500 Series Hardware Specifications sheet](#)

Airwall Gateway/HIPswitch 400

Conductor/Airwall Gateway/HIPswitch 500

Technical Whitepapers, Best Practices, and Use Cases

Additional Resources

Supplementary information that may be useful in managing or deploying the Airwall Solution.

Resource	Link to Download
Outdoor/External Cellular Antenna Reference Guide Suggestions on outdoor/external cellular antennas to use with Airwall Gateways.	Download PDF